

REAL

VNC 4

Viewer

User Guide



Contents

Introduction	3	VNC Viewer options	13
What are VNC Viewer and Server?	3	Colour & Encoding	13
Using VNC Viewer	4	Scaling	14
Making a VNC Viewer connection	4	Identities	14
Scaling the viewer window	5	Inputs	15
Alternative ways to make connections	6	Misc	16
Using the VNC Viewer quick launch icon	6	Load/Save	17
Using the listening VNC Viewer tray icon	6	Browser viewer F8 menu	18
Using a .vnc file to initiate the connection	6	Browser viewer options dialog	19
Using the command-line	6	Using port numbers	20
Making a second connection from an existing one	6	Specifying a port number in VNC Viewer	20
Using a standard web browser	7	Specifying a port number in a browser viewer	20
Viewing a different remote system	8	What is a port?	20
Limitations of VNC Viewer for Java	8	What is an IP address?	21
Using the listening viewer option	9	Assistance	22
Transferring files	10	Troubleshooting	22
Further information	11	Warnings and error messages	22
What is encryption?	11	Support	24
Altering encryption settings	11	Via the web	24
VNC Viewer F8 menu	12	Acknowledgements	24
		Index	25

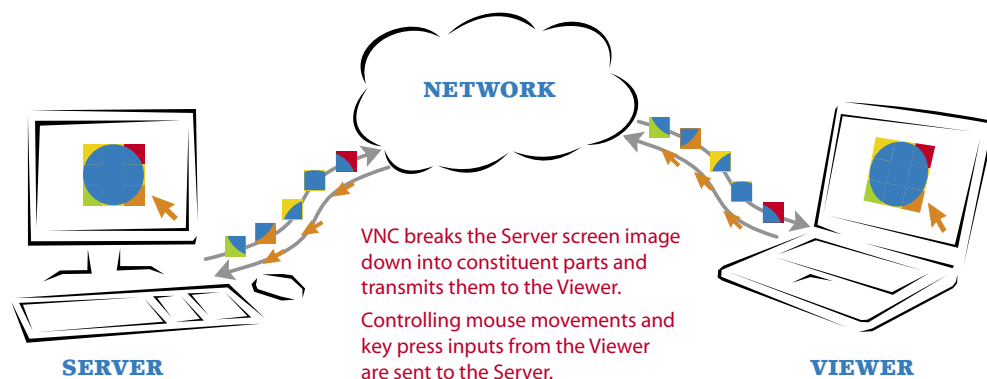
Introduction

What are VNC Viewer and Server?

VNC offers a deceptively simple service - it allows you to view and control a remote system as though seated next to it, wherever you are.

The compact VNC Server 4 application runs on the system to be controlled. Meanwhile, connecting systems can either run the [VNC Viewer application](#) or use a standard [web browser](#) to download and use a Java viewer from the server system.

VNC adapts itself automatically and dynamically to varying conditions, including differing screen contents and network bandwidths. VNC is also platform independent and will happily allow a Windows system to control a Linux server, or vice versa.



Thanks to a comprehensive update VNC now also offers:

- Full user and server authentication ⇔
- [Secure link encryption](#),
- Server [screen scaling](#) to fit any window size.
- File transfer.

User and server authentication

Open network connections pose a number of security challenges and the VNC system has now been updated to provide robust solutions. In addition to the possibility of attackers attempting to gain server access, there is also the chance that false servers can be spoofed to mimic real ones and lure users into disclosing important information. To defend against server attackers, VNC provides secure password protection. To defeat server spoofer, VNC Servers are now required to prove their authenticity by providing a unique identity code before any viewer details are declared. These features are combined with the new high strength link encryption to present a sizeable barrier to attackers.

Using VNC Viewer

Making a VNC Viewer connection

VNC Viewer can be started in a number of ways. See [Alternative ways to make connections](#) for further details.

To make a connection

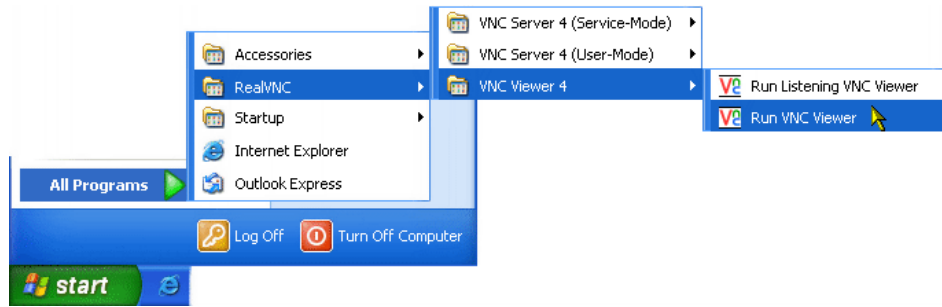
1 Start the VNC Viewer, either:

- Double click the VNC Viewer desktop icon ⇒ 

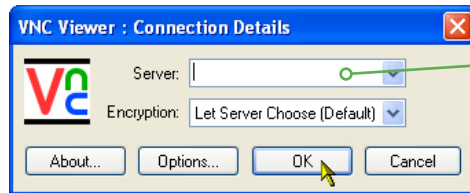
or

i Click the Windows Start button and choose *All Programs* (or *Programs* in non-XP versions).

ii Select the *RealVNC* entry, then *VNC Viewer 4* and finally select *Run VNC Viewer*.



The VNC Viewer connection dialog will be displayed:



Enter the name or IP address of the remote system here

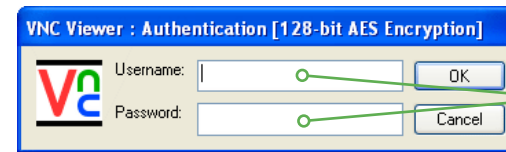
2 Enter the name of the remote system or its [IP address](#) in the *Server* field, or click the down arrow to select one that has been visited previously.

3 Click the *OK* button to connect or optionally:

- [Change the connection options](#)
- [Change the encryption settings](#)
- [Address a server that uses a non-standard port number](#)

4 Depending on circumstances, one or more of the following will happen:

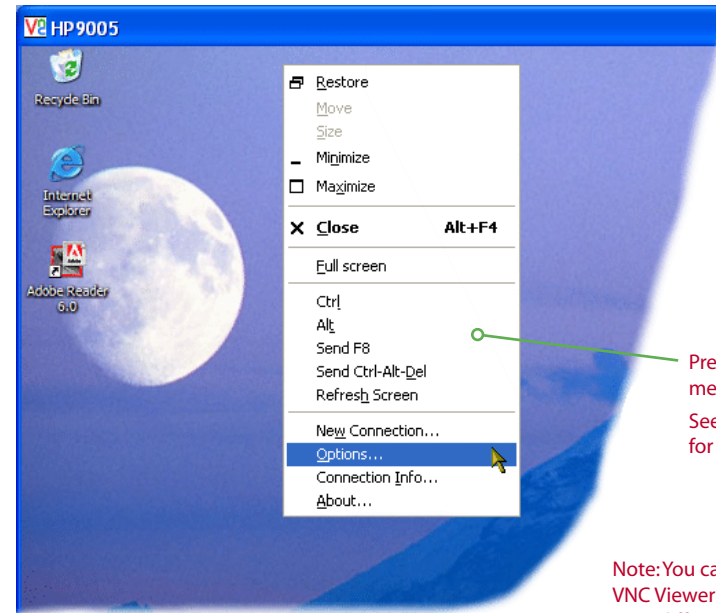
- If the remote system requires authentication, this dialog will be displayed:



Enter a username and password, or just a password if the *Username* field is blanked out. Then click the *OK* button to continue.

- [A warning or error message may be displayed](#), or

- The VNC Viewer window will show the current desktop of the remote system and allow you to control it:



Press F8 to display this menu of options.
See [F8 menu options](#) for details.

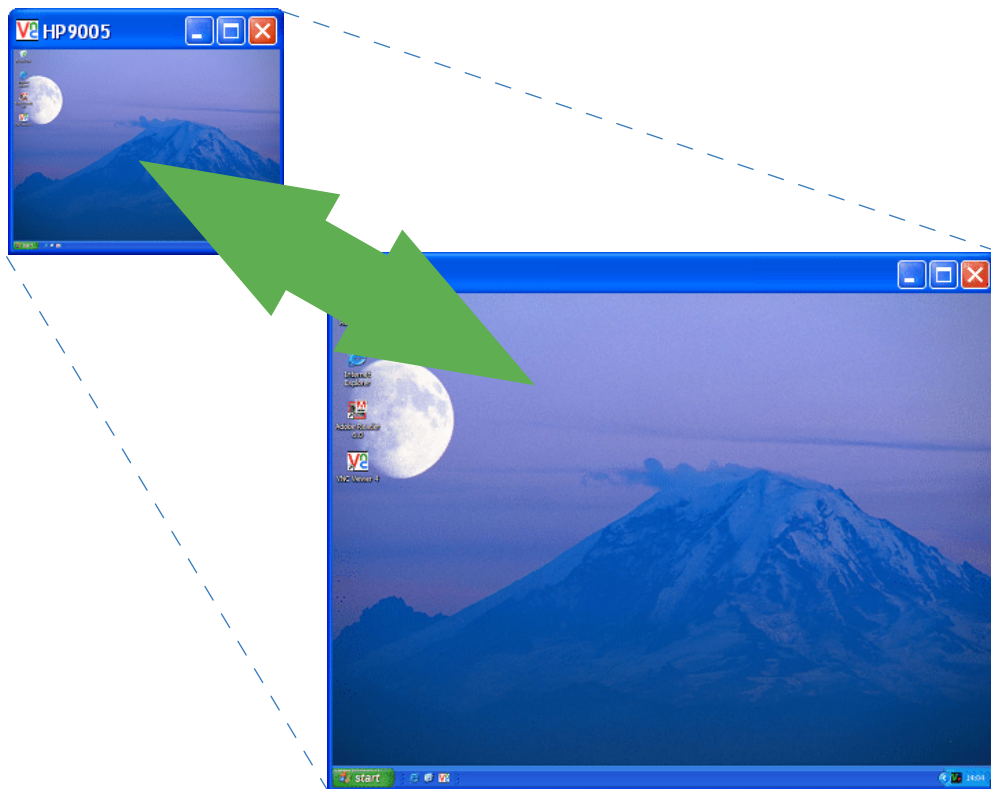
Note: You can run two or more VNC Viewer windows in order to view different remote systems.

To end a connection

- Close the VNC Viewer window.

Scaling the viewer window

VNC Viewer 4 offers a new feature of scaling so that you can alter the overall size of the remote system screen image as it appears on your local viewer system.



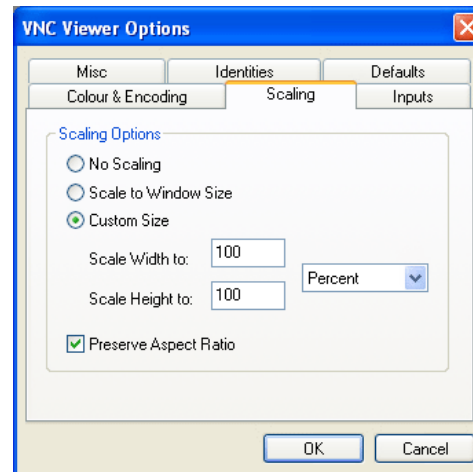
This can be useful in the following situations:

- To reduce a large remote screen resolution to show it in full on a smaller resolution local system,
- To enlarge a small remote screen resolution on a local system for extra clarity,
- To allow multiple VNC connections to remote systems to be displayed simultaneously, side by side.

Scaling is switched off as standard, so you first need to enable it.

To enable the scaling feature

- 1 Display the VNC Viewer Options dialog either:
 - **While making a connection:** Click the *Options...* button in the *Connection details* dialog, or
 - **During a connection:** Press *F8* and select the *Connections...* option.
- 2 Select the *Scaling* tab.



- 3 Choose the required setting:
 - **Scale to Window Size** adjusts the screen image to suit the size of the viewer window. For convenience, if the window size is close to the size of the desktop being viewed, it will snap to that size. You can disable this behaviour by using either the top right or the bottom left corners of the window to resize it.
 - **Custom Size** allows you to select the level of scaling in percentage terms or specify a particular window dimension in pixels.
 - **Preserve Aspect Ratio**, when ticked, ensures that the width and height dimensions remain in the correct ratio.
- 4 Click the *OK* button to accept your changes.
 - **Optionally save scaling as a default:** If you would like scaling to be enabled for every connection, enable it as explained above and then save the defaults - see [Load/Save](#) for details.

Alternative ways to make connections

There are a number of alternative ways to launch VNC Viewer and to make connections with remote systems, as follows:

- Using the VNC Viewer quick launch icon
- Using a *.vnc* file to initiate a connection
- Using the command-line
- Making a second connection from an existing connection
- [Using a standard web browser \(no need for VNC Viewer\)](#)
- [Using the listening viewer option](#)

Using the VNC Viewer quick launch icon

Note: The quick launch icon feature is not available in Windows 95, 98, ME, NT4 or Server 2003.

During the VNC installation, an option was available to create a VNC Viewer quick launch icon. If this option was chosen, then your system will show a VNC icon adjacent to the Start



button:

Simply click the icon to launch VNC Viewer.

If you wish to create a VNC Viewer quick launch icon, click and drag the VNC Viewer entry from the Start menu over the quick launch area. Position the cursor between two existing quick launch icons (a small vertical black line will appear) and then release the mouse button.

Note: If the quick launch area is not visible, use the Windows Control Panel > Task Bar and Start Menu options to enable it.

Using the listening VNC Viewer tray icon

If you are running a listening VNC Viewer then you can make a VNC connection by double-clicking it or by right-clicking on it and selecting the *New Connection...* option. See [Using the listening viewer option](#) for details

Using a *.vnc* file to initiate the connection

A *.vnc* configuration file allows you to store VNC Viewer setup information and connection details so that they can be quickly used again. See [Saving and loading configuration \(.vnc\) files](#) for details about creating a *.vnc* file.

You can use a *.vnc* file, using your mouse, in two main ways:

- **Double click the *.vnc* file.** This will work only if your VNC Viewer was installed using the VNC setup program and is consequently registered within Windows. If so, Windows will start VNC Viewer and apply the details stored within the *.vnc* file.
- **Drag and drop the *.vnc* file onto the VNC Viewer icon.** This will start VNC Viewer and apply the details stored within the *.vnc* file.

*Note: You can also use a *.vnc* file using the command line option, discussed next.*



Using the command-line

You can specify either a server address or a configuration file on the command-line:

- **To specify a server address** simply enter it on the command-line exactly as you would enter it into the Connection dialog, for example “*vncviewer.exe server.domain.com*”.
- **To specify a configuration file** use the *-config* command-line parameter, for example “*vncviewer.exe -config server.vnc*”.

Making a second connection from an existing one

Once VNC Viewer is running and connected to a remote system, it is simple to open further connection windows that can be used to simultaneously view other systems. Note that you can also use any other method of starting VNC Viewer to create a second connection.

Press the F8 key to display the menu and select the *New Connection...* option.

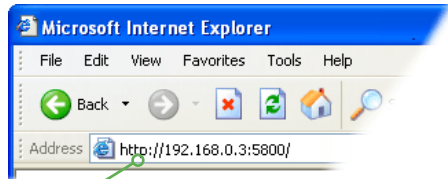
A new *Connection Details* dialog will be displayed. Enter the remote system address and click the OK button.

continued

Using a standard web browser

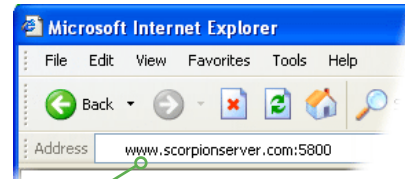
When you need to access your system via a computer that lacks a VNC Viewer (in an Internet café, for instance), the VNC Server program provides a neat feature to give quick and easy access. VNC Server can download a compact Java applet, upon request, to any standard web browser that will temporarily allow it operate in the same way as VNC Viewer.

- 1 Launch your web browser and enter either the IP address or URL of the remote system in the following way:



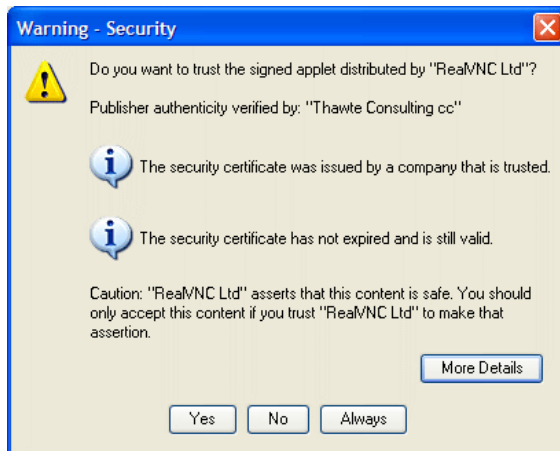
Enter the IP address preceded by `http://` and followed by a colon and then the **port number** used by the remote system - most commonly 5800.

OR



Enter the url, followed by a colon and then the **port number** used by the remote system - most commonly 5800.

- 2 Press *Enter* to accept. If this is a first-time connection to the VNC Server, then your browser will probably ask you to confirm that you trust the Java applet:

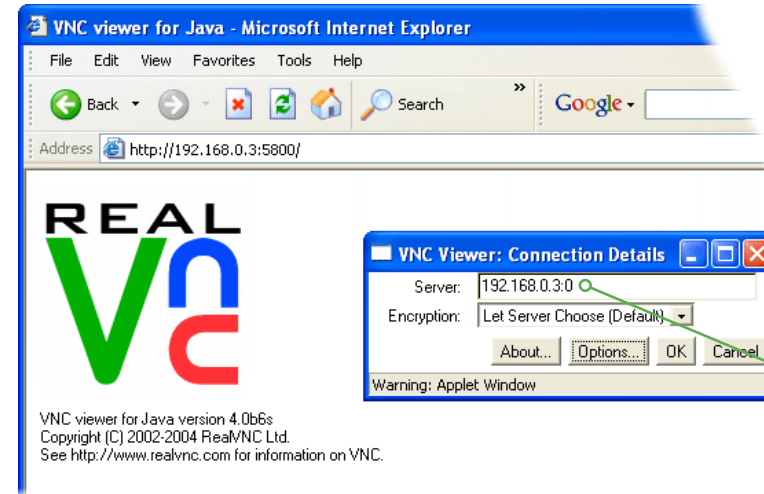


Note: Not all web browsers use versions of Java that support the advanced features described here. If the dialog (shown left) is not displayed during the first connection, then your browser may respond as though you had clicked the *No* button, as described below.

If you answer *No* then the Java applet will still operate, however, some of its advanced features will be unavailable, most notably:

- You will only be able to connect to the VNC Server that supplied the Java applet,
- You will not be able to store the identity of the server to which you are connecting and so will need to reconfirm its signature during any subsequent connections, and
- You will need to use the [F8 menu](#) in order to use the Windows clipboard to transfer information between the local and remote systems.

- 3 Click *Yes*, *No* or *Always*, as appropriate. The remote VNC Server will download the necessary Java applet and then present a *Connection details* dialog:

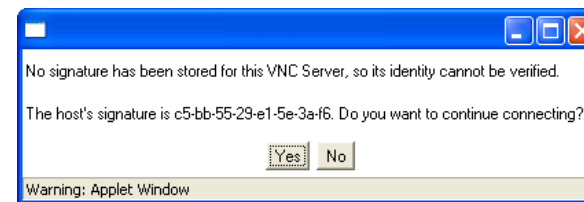


The Server entry should hold the address/name of the remote system entered earlier.

- 4 Click the *OK* button to connect or optionally:

- [Change the Server address to view a different remote system](#)
- [Change the connection options](#)
- [Change the encryption settings](#)

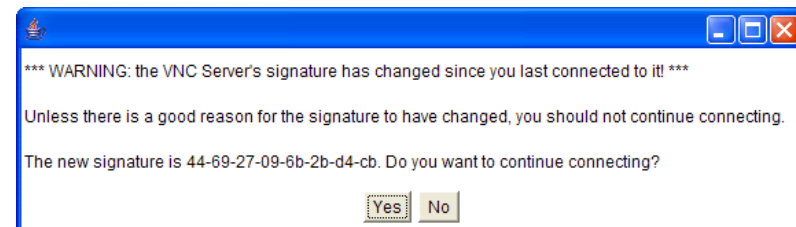
Depending on the configuration of the remote system, the browser may display a confirmation (or a warning) dialog:



↔ The *No signature...* message is displayed if no record of a previous visit is held for this remote system.

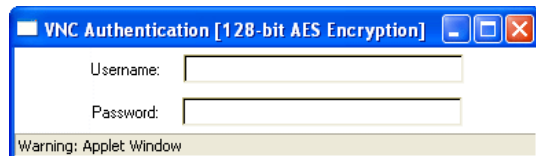
↕ The *Warning* message is displayed if the signature has been changed since the last connection to this remote system.

See [Warnings and error messages](#) for more details about both messages.



- 5 Check the details and if you are confident of the server (see [Warnings and error messages for details](#)), click the *Yes* button.

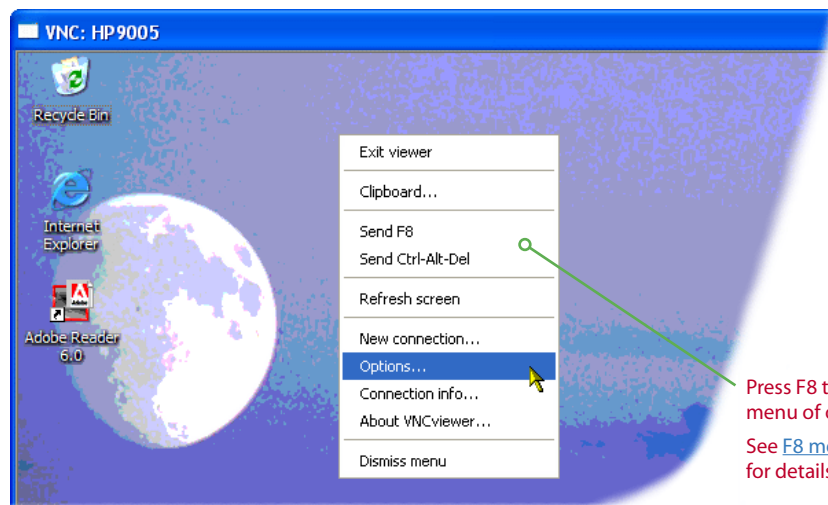
Subject to the security settings of the remote system, the browser may now display an authentication dialog:



Note: When connecting to some systems (just before this dialog is displayed) you may be asked to enter a series of random characters upon which it will base the encryption key. If requested to do this, enter a long string of random characters (the longer and more random the string, the less chance of it being decrypted by a potential attacker).

- 6 Enter a valid *Username* and/or *Password* and press *Enter*.

The viewer window will now be displayed:



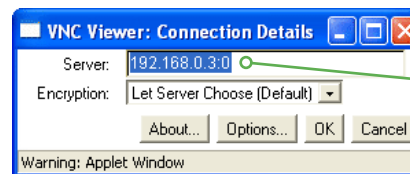
Press F8 to display this menu of options.
See [F8 menu options](#) for details.

Viewing a different remote system

If you accepted the Java applet as trusted (*i.e.* if you clicked *Yes* or *Always* during the initial connection) then you will have the ability to connect with other remote systems running VNC Server, not just the one that supplied the Java applet.

To view a different remote system

- 1 As covered in the [Using a standard web browser](#) section, click either the *Yes* or *Always* buttons to confirm the Java applet as trusted, your browser will display the connection details dialog:



The dialog will initially show the address of the VNC Server system that supplied the Java applet.

- 2 Enter the address of the new remote system that you wish to view and either click the *OK* button or optionally alter other connection settings - see step 4 of the [Using a standard web browser](#) section.

Limitations of VNC Viewer for Java

VNC Viewer for Java supports all the security features of VNC Enterprise Edition such as encryption and server and user authentication. However, it does not currently support scaling or file transfer.

Using the listening viewer option

In certain situations it can be useful to allow a remote system to initiate the connection to your VNC Viewer, rather than the converse. Such instances could include:

- In a demonstration situation (classroom or seminar) where more than one viewer system will simultaneously connect to a single server system.
- Where the firewall protecting the local network of the remote system will not allow incoming connections to be made.

To allow this to occur, your VNC Viewer must be started in a special mode that leaves it dormant within the system tray until an incoming connection is received from a remote VNC Server system. You can start and use VNC Viewer in the usual manner alongside the special listening version.

Note: If the local viewer system is situated behind a firewall (i.e. the remote server system is external to the viewer's local network), then the firewall needs to allow incoming connections at port 5500.

To set VNC Viewer into listening viewer mode

- 1 Click the Windows *Start* button and choose *All Programs* (or *Programs* in non-XP versions).
- 2 Select the *RealVNC* entry, then *VNC Viewer 4* and finally select *Run Listening VNC Viewer*.

A VNC Viewer icon will be added to the Windows system tray area in the lower right corner of the screen:



Listening viewer icon

The listening viewer will remain in this dormant state until a remote system initiates a connection - see opposite.

To stop listening viewer mode

- 1 Right click the listening viewer icon in the system tray.
- 2 In the resulting popup menu, select the *Close Daemon* option.

To initiate a connection to the viewer from the remote system

- 1 On the remote server system, right click on the VNC Server icon in the system tray.
- 2 From the popup menu, click the *Add New Client* option.
- 3 In the resulting popup dialog, enter the IP address of the viewer system and click *OK*. No username or password are required.

A viewer window will open on the local system showing the desktop of the remote server system, exactly as if it had been started in the usual manner.

To end a listening viewer connection

Listening viewer connections can be terminated by either party, either:

- **From the viewer:** Close the viewer window.
- **From the server:** Right click on the VNC Server 4 icon in the system tray and select the *Disconnect Clients* option.

Transferring files

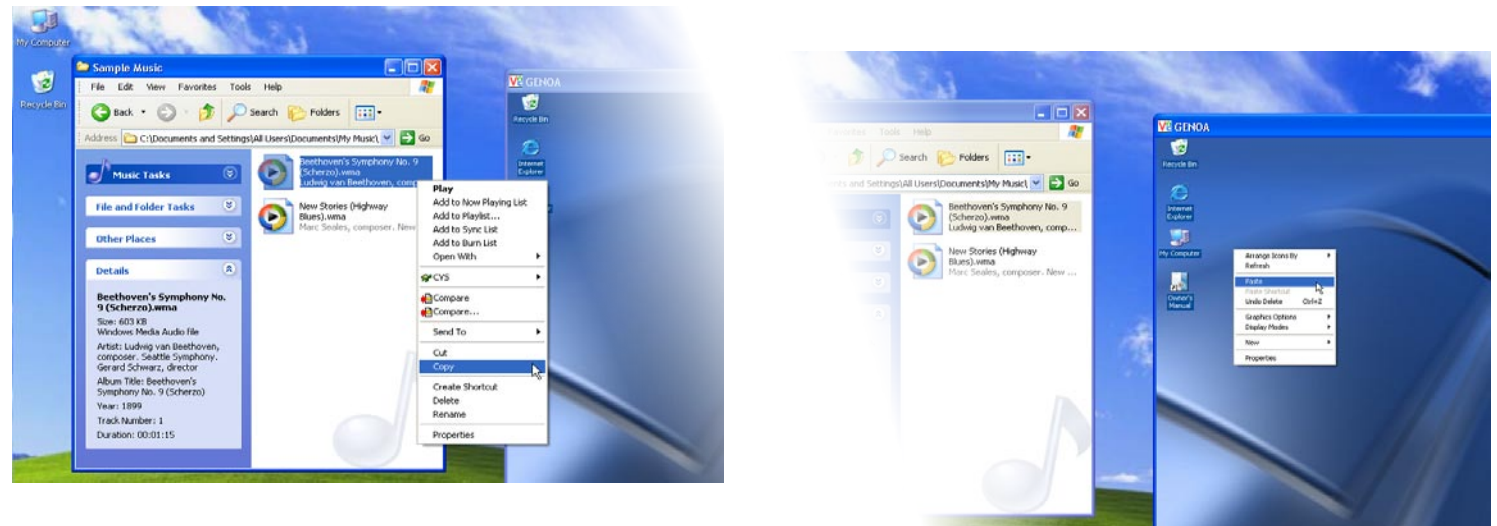
On Windows-based computers, you can transfer files via the clipboard to and from a VNC Server to which you are connected. To copy some files from the computer running VNC Viewer to the computer running VNC Server, do the following:

- Connect to the VNC Server.
- Ensure that both the Server and Viewer components are at least version 4.2. Earlier versions do not support file transfer.
- Ensure that file transfer is enabled. See 'Enable file transfer' for details on how to enable file transfer on the VNC Viewer; see the VNC Server documentation for details on how to enable file transfer on the VNC Server.
- Select the files or folders you want to copy. You can select multiple files at the same time.
- Copy them to the clipboard using either Ctrl+C, or selecting Copy from the Edit menu or from the context (right-click) menu.
- Open the folder into which you want to copy files and paste then using either Ctrl+V or selecting Paste from the Edit menu or from the context menu.

The files will be transferred using the existing VNC connection. Note that you can interact with the VNC session while the copy is in progress, but your files will transfer faster if there is no other network activity while the files are being copied.

It is not currently possible to drag and drop files into or out of the VNC Server desktop. It is also not possible to cut and paste files; if you cut files to the clipboard of the computer running VNC and paste them remotely (or vice versa) then the files will be copied, but will not be deleted from their original location.

Please note that the Java VNC Viewer does not support file transfer.



Further information

This section provides detailed information on a range of subjects related to VNC Viewer 4:

- What is encryption?
- Altering encryption settings
- [VNC Viewer F8 menu](#)
- [VNC Viewer options](#)
 - Colour & Encoding
 - Scaling • Identities
 - Inputs • Misc
 - Load/Save
- [Browser viewer F8 menu](#)
- [Browser viewer options dialog](#)
- [Using port numbers](#)
 - Specifying a port number in VNC Viewer
 - Specifying a port number in a browser viewer
 - What is a port?
- [What is an IP address?](#)

What is encryption?

Network links in general, and the Internet in particular, pose an ever present threat of system spoofing and eavesdropping on connections between systems. The VNC user and server authentication system defeats the former threat, while strong data encryption of the type used by VNC presents a significant barrier to eavesdroppers.

When either the VNC viewer or VNC server enable encryption, both parties exchange codes called *public keys*. From that moment, all information is encrypted prior to transmission, using the other party's public key. As encrypted information is received, the receiving party then uses its matching *private key* to restore the sent information to its original form.

Any eavesdropper who manages to intercept the information flowing between the VNC viewer and server (called a *man-the-middle attack*) will be presented with an unintelligible mess. Even if they were able to capture the public keys, they would still be unable to decode and make sense of the encrypted information.

Due to the calculations that must be performed to codify transmitted information, the use of encryption does impose a slight overhead on performance, estimated to be around 10%.

Altering encryption settings

The *Let Server Choose* option is the default encryption setting for VNC Viewers and defers the decision to encrypt or not, to the remote server system. Many servers in turn, will have their encryption settings configured to *Always On*.

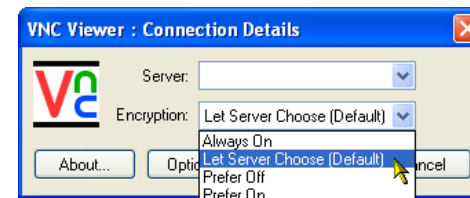
The alternative encryption options available for the viewer are as follows:

- **Always On** ensures that the link is always encrypted. When accessing older versions of VNC Server (that do not support encryption), the use of this setting will cause the connection to be aborted.
- **Prefer Off** requests an unencrypted link but will use encryption if the server insists on it.
- **Prefer On** requests encryption, if the server can support it, but will accept an unencrypted link if the server cannot support it.

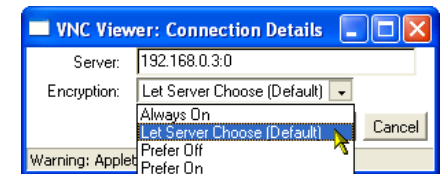
The *Encryption:* box of the *Connection Details* dialog indicates the currently selected setting. After the connection is established, the encryption scheme in use (either *No encryption* or *128-bit AES encryption*) is displayed in the title bar of the authentication dialog and also in the connection details dialog accessible using the F8 menu.

To change the encryption setting

- 1 Using either the [VNC Viewer](#) or a [web browser](#), display the *Connection details* dialog.
- 2 Click the down arrow on the *Encryption* field to display the list of options.



Encryption options within VNC Viewer



Encryption options within the browser viewer

- 3 Select the most appropriate option and continue with the connection process.

VNC Viewer F8 menu

To access the VNC Viewer F8 menu

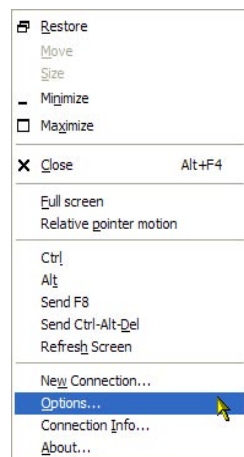
1 Do one of the following, either:

- Press the F8 function key (the F8 setting can be altered to use any of the other function keys, see [VNC Viewer Options](#)),

or

- Right click on the VNC icon in the top left corner of the VNC Viewer window.

The viewer menu will be displayed:



Full screen

Hides the Windows menu bar and VNC Window so that the screen image of the remote system fills the entire local desktop.

Relative pointer motion

In some cases (in particular, when connecting to a hardware-based VNC Server or when remotely accessing an application that interprets mouse pointer input in particular ways) selecting this option can resolve mouse pointer issues. Unless you are experiencing problems with the mouse pointer on the VNC Server, such as excessive pointer acceleration, leave this option disabled.

Ctrl and Alt

These options allow you to enact CTRL and/or ALT keypress sequences (in combination with other keys) on the remote system that would otherwise be interpreted by the local system. For instance, to quickly change between applications on the remote system you need to send ALT and TAB. However, if you press ALT and TAB on the keyboard, then the local system thinks you are talking to it and responds accordingly. If, however, you display the F8 menu, select the Alt option and then press the TAB key, the remote system responds instead (however, see also the VNC Viewer [Inputs](#) options for an alternative method of doing this).

Send F8

This option allows you to send an F8 command to the remote system. This is necessary because F8 is trapped at the VNC Viewer in order to provide access to the F8 menu and is not

passed on to the remote system. If F8 is altered (in [VNC Viewer Options](#)) as the access to the menu, then this menu option changes accordingly.

Send Ctrl-Alt-Del

This option allows you to send the Ctrl Alt-Del key combination to the remote system.

Note: As an alternative to using this menu option, most Windows versions will pass the following keypress sequence to the remote system to achieve the same result: Shift-Ctrl Alt-Del.

Refresh Screen

Requests a complete screen refresh from the remote system.

New Connection...

Displays the Connection dialog to allow a new connection to an alternative system. Note that the connection to the existing remote system will remain unaffected and both (or more) connections can coexist simultaneously.

Options...

Displays the [VNC Viewer Options](#) dialog so that you can make changes to aspects of the current connection.

Note: Certain settings are unchangeable in an existing connection, such as the Shared connection and Protocol options.

Connection Info...

Displays numerous details about the current connection which are mainly of use in support and diagnostic situations.

VNC Viewer options

VNC Viewer options are available either:

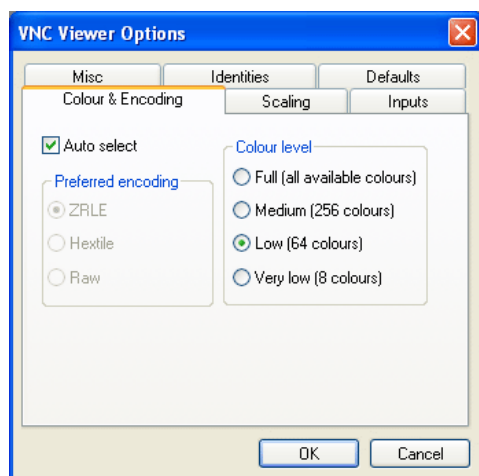
- **While making a connection:** Click the *Options...* button in the *Connection details* dialog), or
- **During a connection:** Press *F8* and select the *Connections...* option.

The Options dialog contains six tabbed pages:

[Colour & Encoding](#) | [Scaling](#) | [Inputs](#) | [Misc](#) | [Identities](#) | [Load/Save](#)

Colour & Encoding

These options determine how the server screen image is transmitted and redrawn.



Auto select

When ticked, the VNC Viewer will automatically check the connection speed to determine the most appropriate method for encoding the remote system screen image and also whether to use full colour.

[Command line equivalent: `AutoSelect=true/false`]

Preferred encoding

The encoding options given here relate to how the screen of the remote system is described and sent to the viewer system. There are various methods available (ZRLE, Hextile and Raw) and each can be specifically selected. However, you are recommended to leave the Auto select option ticked so that the VNC Viewer can select the most appropriate method to match the connection speed.

ZRLE

This method subdivides the remote system screen into many small rectangles which are then individually described. Where adjoining rectangles are of the same colour (*i.e.* in plain backgrounds), each subsequent similar rectangle can simply refer to the last and consequently reduce the information sent. ZRLE uses a high compression rate on all transmitted data and thus, best suits a slower connection such as a modem link. However, more processing is required to decompress and reassemble the received files.

[Command line equivalent: `PreferredEncoding=ZRLE`]

Hextile

This method subdivides the screen information into rectangles in a similar manner to ZRLE, however, it does not compress the information. This means that when it arrives at the viewing system, there is less work for the processor to do in reassembling the screen image. The increase in transmitted data makes Hextile encoding more suitable for faster communication links.

[Command line equivalent: `PreferredEncoding=Hextile`]

Raw

This method simply transmits the remote system screen as a series of decompressed pixel descriptions. This method requires a fast connection speed, however, due to the reduced workload in reassembling the screen data, the performance overhead on the viewer system is lower.

[Command line equivalent: `PreferredEncoding=Raw`]

Colour level

This option allows you to manually select the colour level to use in redrawing the remote system screen. Ranging from Full (all available colours) to Very low (8 colours) the options provide a balance between image quality and network link connection speed.

Note: When the Auto select box is ticked then, dependant on the connection speed, the VNC Viewer may automatically override any manual colour setting and select the Full colour option.

[Command line equivalents:

`FullColour=true/false`

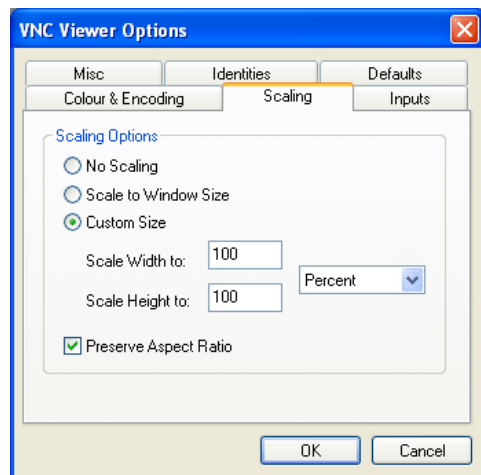
`LowColourLevel=2`

`LowColourLevel=1`

`LowColourLevel=0`]

Scaling

These options provide the ability to reduce or increase the size of a remote system screen when it is displayed on the viewer system. This allows a server screen that uses a high resolution to be displayed in full on a viewer system running at a lower resolution or vice versa.



Scaling options

No Scaling

When selected, the remote system screen is shown unaltered in size within the viewer window.
[Command line equivalent: Scaling=None]

Scale to Window Size

When selected, the remote system screen is dynamically scaled up or down as necessary to fit the size of the VNC Viewer window.

[Command line equivalent: Scaling=Fit or Scaling=AspectFit (to preserve aspect ratio)]

Custom Size

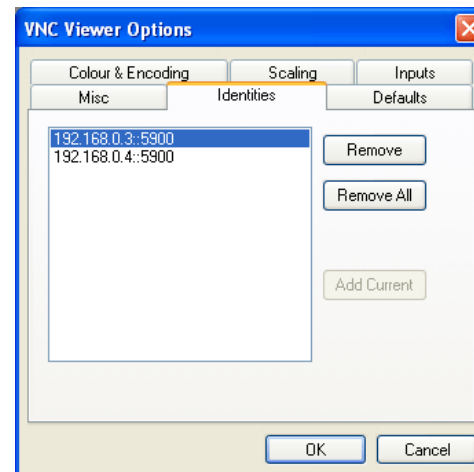
When selected, you can determine the exact level of scaling to apply to the displayed server screen image within the VNC Viewer window. Using the drop down list on the right of the options dialog, you can select the scaling units: *Percent* or *Pixels*. Using either the *Scale Width to:* or *Scale Height to:* edit fields, enter the required scaling figure. If the *Preserve Aspect Ratio* box is ticked, then the other edit field will mimic the value that you enter. Untick the *Preserve Aspect Ratio* box to scale the width and height by different amounts – note that the remote system screen image will be distorted as a result.

[Command line equivalent: Scaling=WWx, xHH, WWxHH, SS% or XX% x YY%]

where: *WW* and *HH* are width and height, respectively, in pixels; *XX* and *YY* are horizontal and vertical scaling factors; and *SS* is an overall scaling factor.

Identities

The identities list contains details of all remote systems that have previously been contacted and provides a known-good reference.



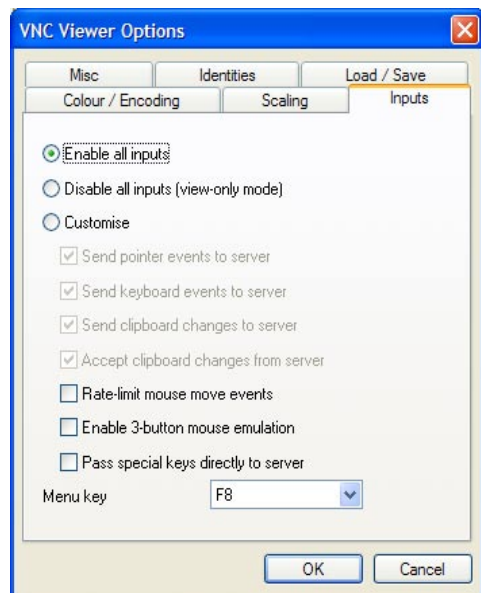
When a connection is made to any remote system, VNC Viewer checks this list and displays a warning if:

- The remote system is not listed (no record of a previous visit), or
- The security key of a remote system has changed since the last visit.

The option buttons given here allow you to *Remove* selected systems, or *Remove All* remote systems from the list. You can also (during a new connection) manually add the current remote system to the list.

Inputs

These options control the information and events that are sent to the server system.



Enable all inputs

If this option is set, then keyboard and pointer events will be sent to the server, and the local and remote clipboard will be synchronised.

Disable all inputs (view-only mode)

If this option is set, then no input will be sent to the server, and the local and remote clipboards will not be synchronised. You will be able to view the remote desktop, but not interact with it.

Customise

This option provides more control over which inputs are sent to the server. You can individually configure the following:

Send pointer events to server

When ticked, the mouse movements of the viewer system are transmitted to the remote system.

[Command line equivalent: SendPointerEvents=true/false]

Send keyboard events to server

When ticked, keyboard inputs on the viewer system are transmitted to the remote system.

[Command line equivalent: SendKeyEvents=true/false]

Send clipboard changes to server

When ticked, an item that is cut or copied to the Windows clipboard of the viewer system is also forwarded to the clipboard of the server. This allows seamless cut, copy and paste operations from the viewer to the remote system. Note that servers can be configured to refuse clipboard data from viewers.

[Command line equivalent: SendCutText=true/false]

Accept clipboard changes from server

When ticked, an item that is cut or copied to the Windows clipboard of the remote system will be accepted into the clipboard of the viewer. This allows seamless cut, copy and paste operations from the server to the viewer. Note that servers can be configured to not send clipboard data to viewers.

[Command line equivalent: AcceptCutText=true/false]

Rate-limit mouse move events

When ticked, mouse movement data will be sent less frequently to the remote system. This can be useful for slow modem connections because information flow is reduced, however, it can result in a noticeable jerkiness to mouse pointer movement.

[Command line equivalent: PointerEventInterval=true/false]

Enable 3-button mouse emulation

When ticked, this option allows you to emulate a 3-button mouse to the remote system using a 2-button mouse at the viewer. To replicate the middle mouse button, simultaneously press the left and right buttons.

[Command line equivalent: Emulate3=true/false]

Pass special keys directly to server

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

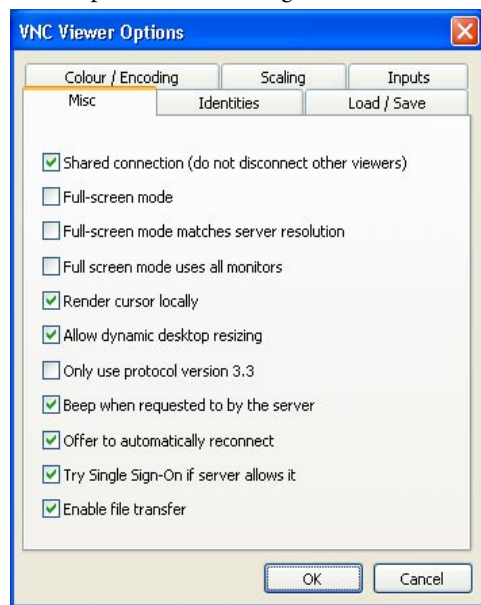
Menu key

Allows you to alter the function key (usually F8) that will display the options menu within the VNC Viewer window. Choose *none* to disable this feature – you can still display the menu using a right click on the viewer window icon in the top left corner.

[Command line equivalent: MenuKey=F8]

Misc

These options cover a range of functions not classified elsewhere.



Shared connection (do not disconnect other viewers)

When ticked, the VNC Viewer will NOT request that any other existing connections to the remote system are terminated. When this option is unticked, depending upon its settings, the remote system may refuse the request to end other connections.

[Command line equivalent: Shared=true/false]

Full-screen mode

When ticked, the VNC Viewer window will open to the full size of the viewer system desktop.

[Command line equivalent: FullScreen=true/false]

Full-screen mode matches server resolution

When ticked, the resolution of the local monitor will be changed to match that of the server when using Full-screen mode. Note that this option cannot be used in conjunction with following option.

[Command line equivalent: FullScreenChangeResolution=true/false]

Full-screen mode uses all monitors

When ticked, all local monitors will be used when using Full-screen mode. Note that this option cannot be used in conjunction with previous option.

[Command line equivalent: UseAllMonitors=true/false]

Render cursor locally

When ticked, the mouse cursor of the remote system is rendered locally by the VNC viewer. This makes the cursor more responsive to mouse movements and is particularly useful when using slower network or modem connections.

[Command line equivalent: UseLocalCursor=true/false]

Allow dynamic desktop resizing

When ticked, the VNC Viewer will accept changes to the resolution/dimensions of the remote system desktop during a live connection. Such changes must be supported by both the server and the viewer to be successful. Disable this option if dynamic changes cause problems on your viewer system.

[Command line equivalent: UseDesktopResize=true/false]

Only use protocol version 3.3

When ticked, causes the viewer to use the original VNC version 3.3 protocol in order to gain compatibility with older VNC server versions. Selecting this option, however, results in an unencrypted link and may cause connection failure to VNC Server versions that insist on a secure connection. *Note: This option cannot be set once a connection has been established.*

[Command line equivalent: Protocol3.3=true/false]

Beep when requested to by the server

When ticked, the viewer system will beep in response to any error beeps emitted by the remote system.

[Command line equivalent: AcceptBell=true/false]

Offer to automatically reconnect

When ticked, the VNC Viewer will offer to reconnect to a remote system whose connection has just been lost. This option does not apply to listening viewer (or reverse, server-initiated) connections.

[Command line equivalent: AutoReconnect=true/false]

Try Single Sign-On if server allows it

When ticked, if the server supports single sign-on, then the user's logon credentials will be presented to the server automatically. If these credentials are refused, then the user will be prompted for a username and password.

[Command line equivalent: SingleSignOn=true/false]

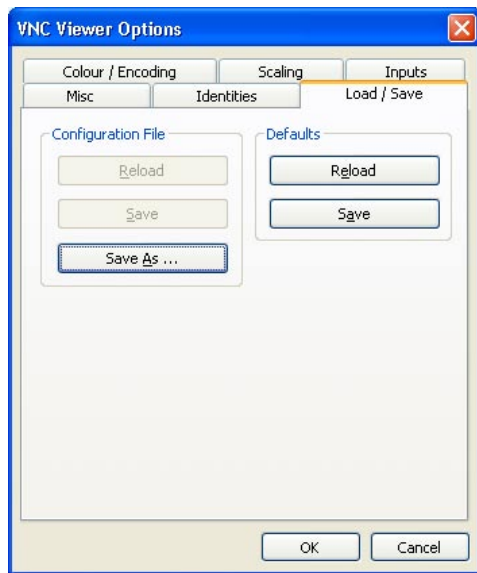
Enable file transfer

When ticked, the VNC Viewer will allow files to be transferred via the clipboard. Note that the corresponding option must also be enabled on the VNC Server to which you are connected. See the VNC Server documentation for details of how to do this.

[Command line equivalent: ShareFiles=true/false]

Load/Save

This page allows you to manage the default options for VNC Viewer so that required settings are available every time a new connection is made. It also controls the creation and reloading of Configuration (.vnc) files that can store specific connection details as well as current settings.



Defaults

Click the *Save* button to set the current settings as the default for the next time you run VNC Viewer. If you don't do this then any configuration changes you make apply only to the current VNC session. Click the *Reload* button to revert all settings to their last saved defaults, or (if they have never been saved) to their original defaults.

Configuration File

VNC Viewer offers the ability to create a configuration file that stores not only the current settings for the viewer but also, if saved during a connection, the connection details, server identity and optionally the password of the remote system. The saved configuration file (which has a .vnc extension) can then be reloaded within the same VNC Viewer or used by other viewers to create replica connections - see [Alternative ways to make connections](#) for details.

To create and reload a configuration file

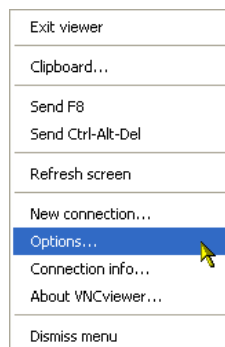
- 1 With a connection established, press *F8* to display the menu.
- 2 Select the *Options...* entry.
- 3 Click the *Defaults* tab.
- 4 Click the *Save Configuration File As...* button. Use the subsequent file dialog to specify a location and name for the new .vnc file.
 - Once the initial file has been created, you can then use the *Save Configuration File* button to save any connection or option changes to the same file.
 - To return to the saved configuration (after further actions have taken place), click the *Reload Configuration File* button.

See [Alternative ways to make connections](#) for details about using a .vnc configuration file to initiate a new connection.

Browser viewer F8 menu

To access the viewer F8 menu

1 Press the *F8* function key. The viewer menu will be displayed:



Exit viewer

Closes the viewer window.

Clipboard...

Displays a VNC Clipboard dialog that allows you to paste items from the local system clipboard and then send them to the remote system.

Note: While making the connection, if you confirmed the Java applet as being trusted, then it is not necessary to use this option. This is because the clipboard will operate as normal between the local and remote systems.

Send F8

This option allows you to send an F8 command to the remote system. This is necessary because F8 is trapped by the viewer in order to provide access to the F8 menu and is not passed on to the remote system.

Send Ctrl-Alt-Del

This option allows you to send the Ctrl-Alt-Del key combination to the remote system. Alternatively, you can use the keypress sequence: Shift-Ctrl-Alt-Del.

Note: As an alternative to using this menu option, most browsers will pass the following keypress sequence to the remote system to achieve the same result: Shift-Ctrl-Alt-Del.

Refresh Screen

Requests a complete screen refresh from the remote system.

New Connection...

Displays the Connection dialog to allow a new connection to an alternative system. Note that the connection to the existing remote system will remain unaffected and both (or more) connections can coexist simultaneously.

Options...

Displays the [Browser viewer options dialog](#) so that you can make changes to aspects of the current connection.

Note: The Shared connection setting is unchangeable in an existing connection.

Connection Info...

Displays numerous details about the current connection which are mainly of use in support and diagnostic situations.

About VNCviewer...

Displays VNC Viewer program and version details.

Dismiss menu

Removes the F8 menu without selecting any option.

Browser viewer options dialog

To access the viewer options menu

- 1 Press the *F8* function key to display the viewer F8 menu.
- 2 Select the *Options...* entry. The options menu dialog will be displayed:

Encoding and Colour Level

Auto select

When ticked, the viewer will automatically check the connection speed to determine the most appropriate method for encoding the remote system screen image.

ZRLE

Select this option to minimise bandwidth use at the cost of increased processing overhead at the viewer and server.

Hextile

Select this option for a good balance of bandwidth use and processing overhead. Hextile typically requires slightly more bandwidth than ZRLE, but the processing overhead is much lower.

Raw

Select this option to send uncompressed pixel data over the network. Processing overhead is minimal, but bandwidth requirements are much higher than the other methods.

Colour level

Select *Full*, *Medium*, *Low* or *Very low*. These options are listed in decreasing order of visual quality and bandwidth requirements.

Inputs

View only (ignore mouse & keyboard)

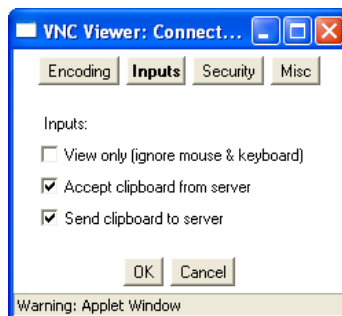
When selected no mouse or keyboard data is sent to the remote system.

Accept clipboard from server

When ticked, items that are cut or copied to the remote clipboard will be made available to the viewer system. Display the F8 menu and select the *Clipboard...* option. Then highlight the data and press *Ctrl X* or *Ctrl C* to cut or copy to the local clipboard, respectively.*

Send clipboard to server

When ticked, you can send items from the local clipboard to that of the remote system. Display the F8 menu and select the *Clipboard...* option. Press *Ctrl V* to paste the local clipboard contents into the dialog and then click the *Send to VNC server* button.*

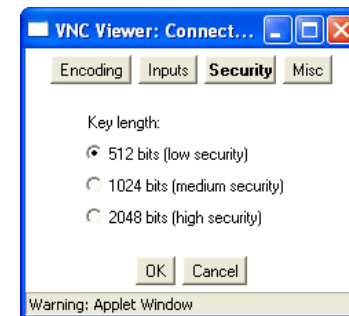


Security

512 bits (low security) - 2048 bits (high security)

This section allows you to determine the encoding strength used for transmitted data. Selecting the high security setting places the highest burden on processing at each system because a private/public key pair must be generated by the browser, which can take a long time for the *2048-bits* option.

Note: In most browsers, this operation is only carried out for the first encrypted connection made; subsequent connections made without closing the browser window will re-use the existing key. In particular, a new key will not be generated for a connection made by selecting 'New Connection' from the F8 menu. Hence, the use of 2048-bit encryption is recommended for maximum security on all but very slow computers.



Misc

Shared connection (don't disconnect other viewers)

When ticked, the viewer will NOT request that any other existing connections to the remote system are terminated. When this option is unticked, depending upon its settings, the remote system may refuse the request to end other connections.

Render cursor locally

When ticked, the mouse cursor of the remote system is rendered locally by the viewer. This makes the cursor more responsive to mouse movements and is particularly useful when using slower network or modem connections.

Fast CopyRect

When ticked, operations such as window dragging are handled as efficiently as possible. However, under some Java virtual machines, this can give visual artifacts. In such cases, try disabling this option.



* If the Java applet is trusted (see [page 6](#) for details), it will be able to link into the Windows clipboard and so the F8 menu function will not be required pass data from system to system.

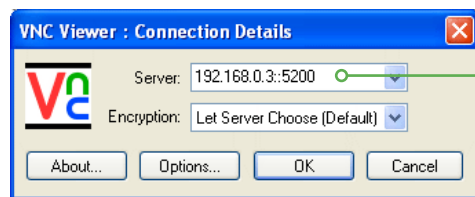
Using port numbers

Specifying a port number in VNC Viewer

When using VNC Viewer you should not normally need to enter a port number, only the address of the remote server system. This is because the majority of VNC Server installations use the standard port number of 5900 and all VNC Viewers are configured by default to use that number. The only time that a port number will be required is when a remote system is configured to an alternative number.

To specify a non-standard port number in VNC Viewer

- 1 Contact the administrator to discover the address and port number of the remote system.
- 2 [Display the Connection details dialog](#) in the usual manner.
- 3 Enter the address (IP address or url) of the remote server system, immediately followed by **two colons** and then the port number:



Enter the address, then *two colons* and then the non-standard port number (in this case 5200). Alternatively, you can express the port as a desktop number - see below right.

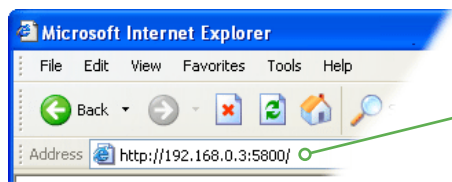
- 4 [Proceed with the connection](#) the usual manner.

Specifying a port number in a browser viewer

When you use a browser to connect to a remote system, the initial connection is always to an alternate port where the server will provide the necessary Java applet to the browser. Once the Java applet is running on the viewer system, the actual viewing session will then switch to the main port number used by the server (usually 5900). Whenever you use a browser, you must always specify the initial Java port number - most VNC Server installations use port 5800.

To specify the port number in a browser viewer

- 1 Contact the administrator to discover the address and port number of the remote system.
- 2 Launch your web browser.
- 3 Enter the address (IP address or url) of the remote server system, immediately followed by **one colon** and then the port number:



Enter the address, then *one colon* and then the port number where the Java viewer applet will be served (usually 5800)

- 4 [Proceed with the connection](#) the usual manner.

What is a port?

Not to be confused with a physical port (such as a USB port or a printer port) to which you connect devices, a *Port* in this context could be more accurately described as a '*service contact-point*'. It is used to help define the kind of data that are being transmitted and, as a result, how to channel them.

Imagine the problem that exists for networking equipment. A disparate mixture of messages and information are continually flowing from system to system, via gateways and routers, and each needs to find the correct destination. In this process, the [IP address](#) plays a critical role in making sure that the right items arrive at the right places, however, the unsung hero is definitely the port number. While the IP address directs the postman to the correct building, it's the port number that gets the package through the door of the correct apartment. Without the port number, there would be piles of unclaimed packages filling the foyer.

Every application that sends or receives information across a network uses a port number. In many cases they are fixed numbers that are always used by particular applications, and because they are not often changed, they are not normally mentioned. For instance, if you send an email (via the most common method), then your message will be marked with port number 25. Whenever you browse the Web, the information will always be denoted with port number 80 and VNC applications almost always send and receive using port number 5900. The systems at the receiving end then know to route messages marked as port 25 to the email server, port 80 to the web server, port 5900 to the VNC server and so on.

Desktop numbers

An alternative way to express a port number is as a *desktop number*. Desktop numbers represent ports that lie in the range 5900 to 5999 and require a *single* colon followed by a number between 0 to 99. Thus, a connection to *my_machine::5902* can equally be expressed as *my_machine:2*. Desktop numbers are important when connecting to UNIX VNC Servers.

What is an IP address?

An *IP address* is a unique identity given to every device connected to a network of any size: from a two system link up at home, to every system on the Internet.

IP addresses are written as four decimal numbers separated by full stops, such as *192.168.0.4*. This is called *dotted decimal notation* and is used as a means of concealing the equivalent real address that is actually used by computers and networking equipment. The bare truth is that every IP address is really a pattern of 32 ones and zeroes.

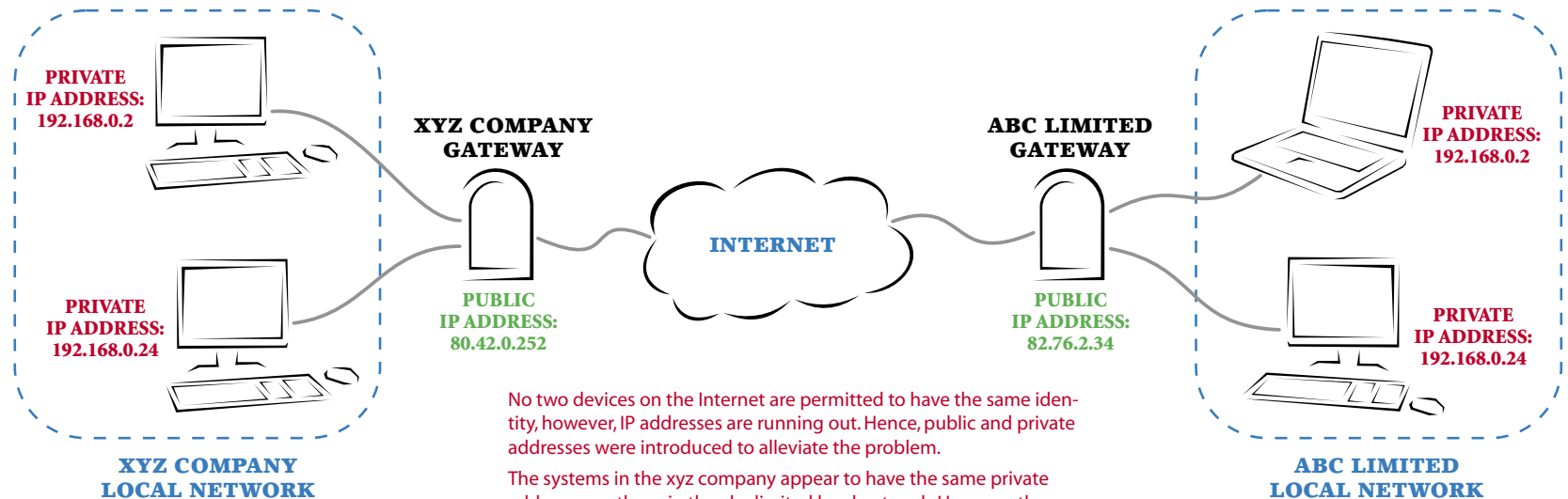
At the inception of the Internet in the 1960s and 1970s, even by wildest estimates, no one ever expected they would need more than the seemingly inexhaustible 4.2 billion unique address patterns that are afforded by 32 ones and zeroes. However, two factors conspired to prove this to be wrong: Firstly, the amazing proliferation and expansion of the Internet; and secondly, the rather inefficient way in which those addresses were originally handed out to organisations and companies. The result was that by the early 1990s, it was already apparent that at the projected growth rates, the reserve of 4.2 billion addresses would soon all be gone.

In order to prolong the current stocks of numbers, the allocation of addresses was greatly tightened and the idea of *public* and *private* addresses was introduced. In the opening sentence here, it was stated that an IP address is a unique identity - this no longer strictly true.

Of the 4.2 billion possible addresses, almost all of them are still used as unique *public* addresses. However, in the revised plan, three groups of addresses were held aside for use as *private* addresses:

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

To avoid confusion, these ranges are never used as public addresses.



No two devices on the Internet are permitted to have the same identity, however, IP addresses are running out. Hence, public and private addresses were introduced to alleviate the problem.

The systems in the xyz company appear to have the same private addresses as those in the abc limited local network. However, there is no ambiguity because to the outside world, they use the public addresses of their gateways. Their gateways handle all of the address translation and ensure that the private addresses never leak out onto the wider Internet.

Now, when xyz company needs to connect their many internal computers to the Internet, they might only be given a single public address, say *80.42.0.252*. They would then connect a *Gateway* system to the Internet and give it that unique public address. Situated on the other side of that gateway would be the company's local network and every system in that local network would receive a private IP address. For small local networks, the most common private address range is that which starts at *192.168.0.0*.

Every computer in the local network (or *subnet*) will use their number that is unique to them within the local network. However, the public identity for all of those local systems, as they pass information out across the Internet, will always be that of the gateway: *80.42.0.252*. It is the job of the gateway to translate addresses between the local and wider networks. The gateway must ensure that messages and data are sent through to the correct locations without the private addresses ever leaking out. Assisting with this task are the *subnet mask* and [port numbers](#). In this way, there are now many systems using similar private IP addresses, however, because those numbers only ever exist in local domains, there is never any confusion.

Of course, most people never see an IP address. To make network addresses even more memorable than the dotted decimal notations (which in turn are used to hide the true binary values), they are usually converted into named addresses. Such conversions are handled by the Domain Name System and your browser uses it every time you visit a web site.

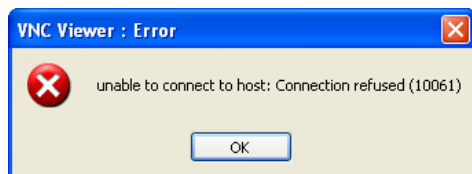
Assistance

Troubleshooting

Warnings and error messages

When connecting to remote systems there are a number of messages that may be displayed depending on the varying circumstances. This section aims to explain the most common messages that you may encounter.

Connection refused (10061)



This error indicates that the IP address entered into VNC viewer was valid and contactable, but that nothing was accepting connections on the default port. The most likely causes are:

- An incorrect address has been entered for the remote system,
- VNC Server is not running or is not accepting connections,
- VNC Server is configured to use a [non-standard port number](#).

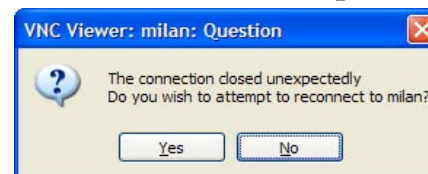
Connection timed out (10060)



This error indicates that no response was received from the VNC server, even to reject the connection. It may be caused by network failure, but the most common causes are:

- Trying to connect to a VNC Server that is behind a NAT router using its private IP address,
- Trying to connect to a VNC Server that is behind a NAT router without setting up the appropriate port forwarding. See your router's documentation for details on how to set up port forwarding.
- Trying to connect to a VNC Server that is behind a firewall that has not been configured to allow VNC traffic through. See the section entitled Dealing with firewalls in the VNC Server documentation for more details.

Connection closed unexpectedly



This error indicates that the IP address entered into VNC viewer was valid and contactable and that something accepted the connection, but the connection was closed without reporting a specific error message. Check the following:

- Does the error persist if you click Yes?
- Is the VNC server running and accepting connections on the port you're trying to connect to?
- Is the access control of the VNC server is configured to allow access from the IP address of the computer you're connecting from? The default configuration does not restrict access based on IP address.
- Are there any error messages logged to the [application event log](#) of the computer running VNC server? If so, please include this information if you need to submit a support request.
- Is the application event log full on the computer running VNC server? If so then empty it or configure it to overwrite old entries.

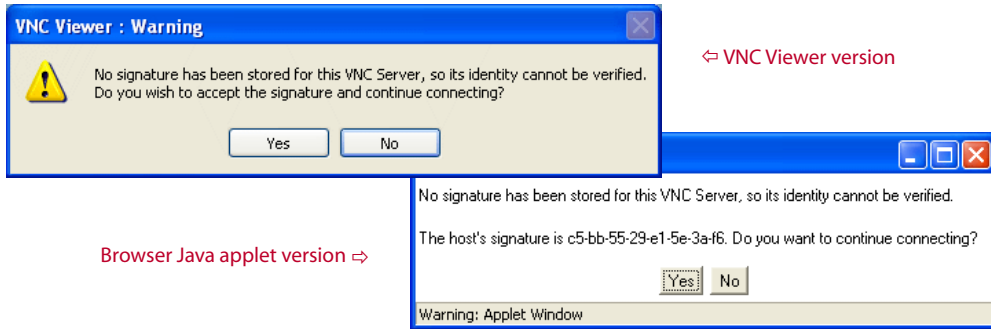
No matching security types



Possible cause:

- The remote system does not support encryption (possibly an earlier version or a Free Edition of VNC Server) but your VNC Viewer is demanding an encrypted link, or *vice versa*.

To remedy this situation either, upgrade the remote system to a higher version of VNC Server, or [change the Encryption setting](#) on your VNC Viewer to *Let Server Choose* and try to reconnect (*Caution: the resulting link will be unencrypted*).

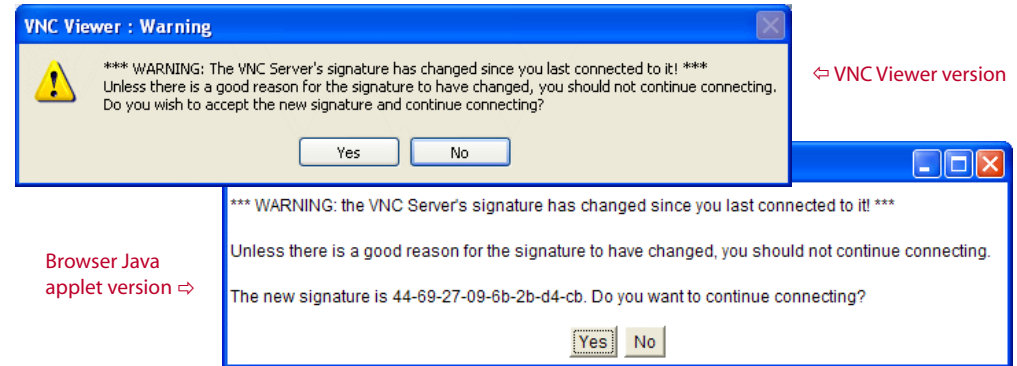


No record of a previous signature

This message indicates that no record exists of a previous connection to the remote system to which you are attempting to connect. The cause of this could be:

- You have not previously visited the remote system, or
- The record of a previous visit to the remote system has been removed from the Identities list within VNC Viewer options.
- This is the first time you have visited the remote system since upgrading from VNC Viewer 4.1.6 or earlier. From version 4.1.7, VNC Viewer uses a more robust mechanism for identifying hosts which unfortunately is incompatible with that used by earlier versions.

If you proceed with the connection then it will be added to the Identities list and no further warnings will be given when making future connections.



Signature has changed

This message indicates that the remote system, to which you are attempting to connect, has undergone a change within its core security settings since your last visit. The causes of this could be:

- The security key of the remote system has been changed, or
- Another system may be masquerading as the one to which you are connecting.

If you have concerns for the validity of the remote system, do not proceed:

- First contact the administrator or user of that system to ascertain whether any configuration changes have been made.

Support

If you are unable to solve your problem after checking through the Troubleshooting section in this guide, please take a look at our on-line [FAQ page](#) and also the [Known Bugs & Features](#) section of the RealVNC website.

If you still cannot find a solution, then please contact us for further assistance:

Via the web

The www.realvnc.com website offers a number ways to gain assistance regarding VNC products:

Search indexes

Provides an opportunity to search through the various VNC databases for solutions.

www.realvnc.com/swish-e/search

Mailing lists

Real VNC provide discussion forums for important announcements and many other VNC-related subjects. You can browse or search previous discussion entries, or alternatively subscribe to one or more forums.

www.realvnc.com/lists.html

Product support request

This section lets you to send queries directly to a VNC support representative.

www.realvnc.com/support.html

Please include as much information as possible regarding the problem, including the exact text of any error messages you see (including the error number) and what you're doing when you see them. Please also include the version of VNC server and VNC viewer that you are using, and what operating system you are running at both ends of the connection.

Acknowledgements

VNC Viewer contains software from more than one source. For full details of this software and the terms under which it is distributed, see the RealVNC website.

www.realvnc.com/products/personal/4.2/acknowledgements.html

Documentation by:  www.ctxd.com

Index

A

- Address
 - entering in a browser 7
- Attack
 - man-in-the-middle 11
- Authentication
 - browser viewer 8
 - VNC Viewer 4

B

- Browser
 - making a connection 7

C

- Colour & Encoding
 - tab 13
- Configuration files
 - using .vnc to start connection 6
- Connection
 - alternative methods 6
 - end 4
 - second 6
- Connection details
 - browser 7
 - VNC Viewer 4

E

- Encryption
 - settings 11
- End connection 4
- Error messages 22

F

- F8 menu
 - browser 18
 - VNC Viewer 4, 12
- FAQ 24

H

- Hextile
 - encoding 13

I

- Icon
 - desktop 4
 - quick launch 6
- Identities
 - tab 14
- Inputs
 - tab 15
- IP address
 - entering in a browser 7
 - entering in VNC Viewer 4
 - what is it? 21

J

- Java
 - applet 7

L

- Listening viewer 9

M

- Menu
 - F8 - browser 18
 - F8 - VNC Viewer 12
- Misc
 - tab 16

O

- Options
 - browser 19
 - VNC Viewer 13

P

- Password
 - browser connection 8
 - VNC Viewer connection 4
- Port
 - what is it? 20

Q

- Quick launch icon 6

R

- Raw
 - encoding 13

S

- Scaling
 - tab 14
 - window size 5
- Support 24
 - getting assistance 24

T

- Tabs
 - Colour & Encoding 13
 - Identities 14
 - Inputs 15
 - Misc 16
 - Scaling 14

U

- URL
 - entering in a browser 7
- Username
 - browser connection 8
 - VNC Viewer connection 4

V

- Viewer
 - listening 9
- VNC Viewer icon 4

W

- Warnings 22
- Web browser
 - using 7

Z

- ZRLE
 - encoding 13