Contents

Document Conventions 2
   Software Versions 2

Introduction 3
   What are VNC Viewer and Server? 3

Using VNC Viewer 4
   Making a VNC Viewer connection 4
   Scaling the viewer window 5
   Alternative ways to make connections 6
      Using the VNC Viewer quick launch icon 6
      Using a .vnc file to initiate the connection 6
      Making a second connection from an existing one 6
      Using a standard web browser 7
      Viewing a different remote system 8
      Using the listening viewer option 9

Further information 10
   Altering encryption settings 11
   VNC Viewer F8 menu 12
   VNC Viewer options 13
      Colour & Encoding 13
      Scaling 14
      Identities 14
      Inputs 15
      Misc 16
      Defaults 17
   Browser viewer F8 menu 18
   Browser viewer options dialog 19
   Using port numbers 20
      Specifying a port number in VNC Viewer 20
      Specifying a port number in a browser viewer 20
      What is a port? 20
      What is an IP address? 21

Assistance 22
   Troubleshooting 22
      Warnings and error messages 22
   Support 24
      Via the web 24
      By post 24

Index 25
Document Conventions

Software Versions

This document covers all versions of VNC Viewer Enterprise Edition from version 4.1, and all versions of VNC Viewer Personal Edition. However, it includes features that are not available in all versions. Where the operation or user interface of the software has changed substantially, this is marked in the text using a coloured background as follows:

The feature described was added in VNC Viewer Enterprise Edition version 4.1.4, or has changed substantially between versions 4.1.3 and 4.1.4. All such features are also available in all versions of VNC Viewer Personal Edition.

The feature described was added in VNC Viewer Enterprise Edition version 4.1.7, or has changed substantially between versions 4.1.4 and 4.1.7. All such features are also available in VNC Viewer Personal Edition version 4.1.2.
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.

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

2. Depending on circumstances, one or more of the following will happen:
   - If the remote system requires authentication, this dialog will be displayed:

   ![VNC Viewer connection dialog]

   - 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:

   ![VNC Viewer window]

3. 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.

4. 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

To end a connection
- Close the VNC Viewer window.

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

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 Defaults for details.

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.
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
- 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:

![VNC Viewer quick launch icon]

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 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.

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 to 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 preceeded by http:// and followed by a colon and then the port number used by the remote system - most commonly 5800.
   - 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:

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:

   - 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:

![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:

![Viewer window]

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:

![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.
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.
Further information

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

• Altering encryption settings
• VNC Viewer F8 menu
• VNC Viewer options
  Colour & Encoding
  Scaling • Identities
  Inputs • Misc
  Defaults
• 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?
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.
3. Select the most appropriate option and continue with the connection process.

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-in-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%.
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),
   - 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 allows 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
- Defaults

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 back-
grounds), 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 uncompress 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 view-
ing 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 uncompressed 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%xYY%]
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.

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 functions not classified elsewhere.

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 problem 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. IMPORTANT: Prior to version 4.1.7, if the VNC server is running on Windows NT 4 and the VNC viewer is running on any other platform, then this option must be disabled, otherwise the connection will be refused. This is due to a limitation of Windows NT 4.
**Defaults**

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.

**Reload Defaults**

Click this button to return the VNC Viewer options to their settings as determined when they were last saved, or (if they have never been saved) to their original defaults.

**Save As Defaults**

Click this button to take a snapshot of the current option settings. These new default settings will then be used every time VNC Viewer is restarted or re-imposed when the Reload Defaults button is clicked.

**Saving and loading configuration (.vnc) files**

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 will include 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.
Browser viewer F8 menu

To access the viewer F8 menu

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 allows 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.

Refresh Screen
Requests a complete screen refresh from the remote system.

New Connection...
Displays the Connection dialog to allows 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**
This method 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 uncompress and reassemble the received files.

**Hextile**
This method produces more data than the ZRLE option and so does not favour a slower link. However, a lower workload is placed on the viewer system in reassembling the screen image.

**Raw**
This method transmits the remote system screen data as pixels. This method requires a fast connection, but places a very low overhead on the viewer system.

**Colour level**
Currently, only the Medium (256 colours) option is supported.

**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 Windows clipboard of the remote system 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.*

**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.

**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.*

* 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 where 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 the 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)

Possible causes:
- VNC Server is not running or the remote system does not exist,
- An incorrect address has been entered for the remote system,
- VNC Server on the remote system is configured to use a non-standard port number.

Connection timed out (10060)

Possible causes:
- 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

Possible cause:
- This error will always have an accompanying entry in the Application Event Log of the host on which the VNC Server is running. This entry will begin with the text “Connections: closed” and will include details of why the connection was closed.
If this is a transient error, then you may be able to reconnect simply by clicking Yes.

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.
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 the VNC development team.

www.realvnc.com/cgi-bin/support.cgi

By post

RealVNC Limited
17d Sturton Street
Cambridge
CB1 2SN
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 saving and loading 17 using .vnc to start connection 6
Connection alternative methods 6 end 4 second 6
Connection details browser 7 VNC Viewer 4

D
Defaults tab 17

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 window size 5
Support getting assistance 24

T
Tabs Colour & Encoding 13 Defaults 17 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