REAL VNC

VNC Server 4.4

Enterprise Edition

User Guide

Copyright and Confidentiality

Copyright Statement

Copyright © RealVNC Ltd, 2008. All rights reserved.

No part of this documentation may be reproduced in any form or by any means or be used to make any derivative work (including translation, transformation or adaptation) without explicit written consent of RealVNC.

Confidentiality Statement

All information contained in this document is provided in commercial confidence for the sole purpose of use by an authorised user in conjunction with RealVNC's products. The pages of this document shall not be copied, published, or disclosed wholly or in part to any party without RealVNC prior permission in writing, and shall be held in safe custody. These obligations shall not apply to information which is published or becomes known legitimately from some source other than RealVNC.

Registered office:

VNC House,

Sturton Street,

Cambridge,

CB1 2SN

United Kingdom

www.realvnc.com

Contents

Introduction to VNC

Virtual Network Computing (VNC) is remote desktop access software which allows one computer (the *viewer*) to take full control of another (the *server*), whether on a local network or anywhere in the world over the internet. The computers don't even have to share the same operating system; for example, you could use VNC to view and control a Windows Vista desktop at the work, by using a Linux or Mac computer at home. Applications of VNC include remote access, home-working, remote maintenance, helpdesks and business collaboration.

As shown in the diagram below, VNC consists of a server and a viewer:

- The *VNC Server* is the software application on the computer to be remotely accessed.
- The *VNC Viewer* is the software application that watches and interacts with the VNC server on the remote computer.

This guide provides information on the installation, configuration, and use of VNC Server. For detailed information on the VNC Viewer, please see the separate user guide.

Security concerns

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 "spoof" or mimic real ones and lure users into disclosing important information. To defend against server attackers, VNC Server Enterprise Edition provides secure password protection. To defeat server "spoofers", 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.

VNC link 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 Enterprise Edition authentication system

defeats the former threat, while strong data encryption of the type used by VNC presents a significant barrier to eavesdroppers. When either VNC Viewer or VNC server enable encryption, both parties exchange codes called encryption. From that moment, all information is encrypted prior to transmission.

VNC Server Operating modes

When you install VNC Enterprise Edition, 2 operating modes will be available:

- Service Mode (Default)
- User Mode

Service Mode

This is the most commonly used mode. VNC Server starts in this mode by default.

Service Mode is suited to a system administrator controlled, multi-user environment where users frequently need to offer remote access to their computers. In Service mode, VNC Enterprise Edition operates in the following way:

- Is available as soon as the system has started up.
- Is available even when the user has logged out, or if the computer is locked.
- Is configured with a single set of system-wide options.

User Mode

User Mode is suitable for a **single** user who may require occasional help from a remote third party, and infrequently shares work. In user mode, VNC Enterprise Edition operates in the following way:

- Runs as a normal application, according to the current user's system rights.
- Is not available when the user logs out, or if the system is locked.
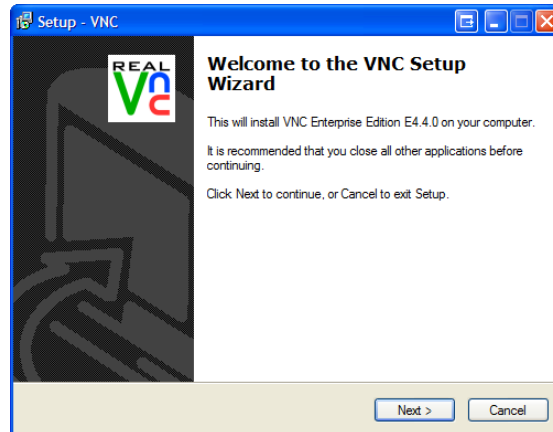- Can be configured by each user independently.

Installation & Setup

VNC Enterprise Edition is available as a self-extracting installer, and can be downloaded from

www.realvnc.com

Once you have downloaded the exe, follow these steps to install the application.
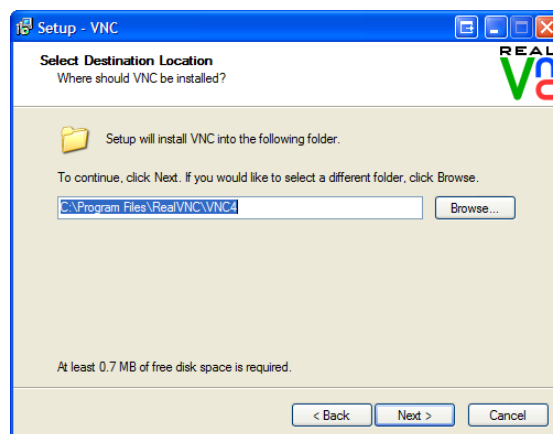
1. Double-click on **vnc-E4_4_0-x86_x64_win32.exe**, to start the installation:


2. Click **Next** to continue. This displays the License Agreement:
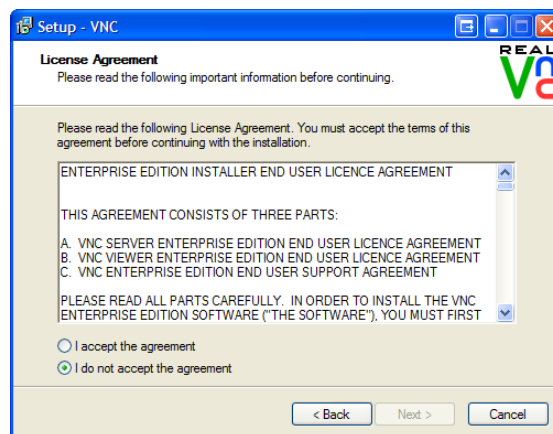
3. Please read the license agreement, click the "**I accept the agreement**" check box, and then click **Next**. The next dialog will prompt you to choose an installation folder for the RealVNC software:

4. If you would like to choose an alternate installation folder, click **Browse** to select. Otherwise, click **Next**. This displays the Select Components dialog:
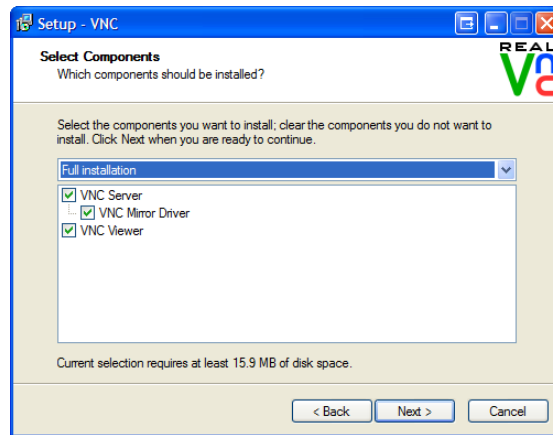
5. By default, VNC Server, VNC Mirror Driver, VNC Viewer and Documentation will be installed. If you don't want to install any of these options, click the check boxes to de-select them, and then click **Next**.
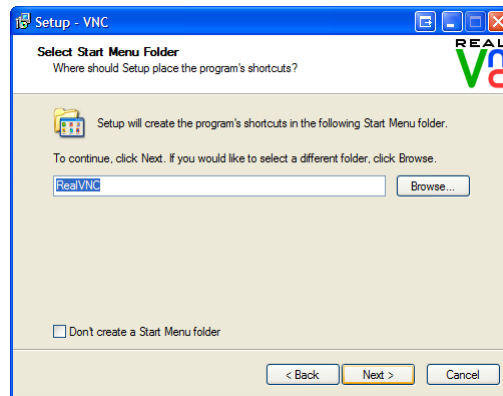
6. If you would like to choose an alternate installation folder, click **Browse** to select. To accept the suggested folder, click **Next**.

    NB: To avoid adding a RealVNC entry in your Start menu, click the "**Don't create a Start Menu folder**" checkbox.
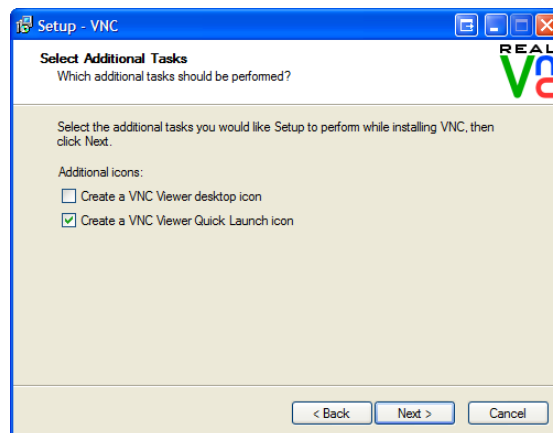
7. If you would like to create Desktop and Quick Launch bar icons, click the appropriate checkboxes, and then click **Next**.

The Ready to Install dialog is displayed, which lists all of the components to be installed.
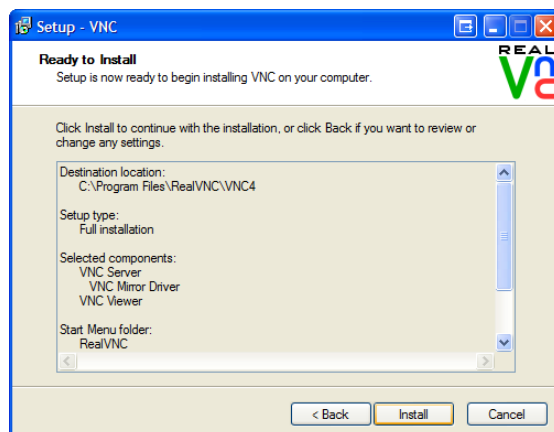
8.   To begin the installation, click **Install**. A progress bar will be displayed during installation.

9.   Click **Next**. When installation and setup have completed, the following dialog is displayed:
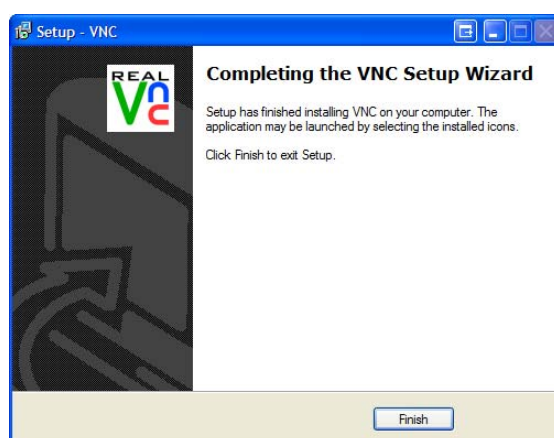
10.   Click **Finish** to exit the Setup Wizard, and to start the VNC Server Service.

The VNC Server will start, by default in Service Mode, and the *VNC Server Status* dialog will be displayed:
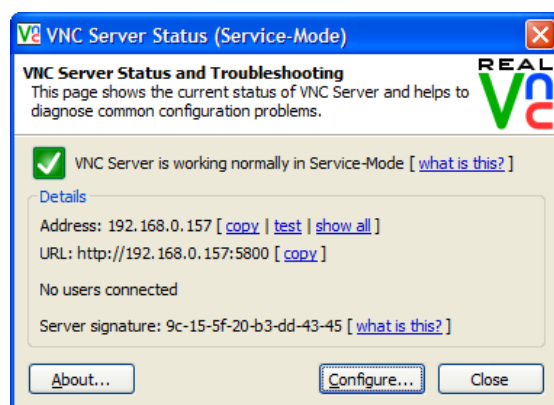
The VNC Server Status dialog shows the current status of the VNC Server, your current IP Address, the number of users connected to your VNC Server, and the VNC Server signature.

VNC Server is now ready to use.

For further configuration options, refer to the Configuration section.

Configuration

You can optimise VNC Server for particular types of use; this section will focus on the following:

- Maximum security required
- Maximum speed is required
- Server demonstration to a group

The VNC Server configuration can be edited at any time by clicking **Configure** on the VNC Server Status dialog.

To display the VNC Server Status dialog

On the windows task tray, double-click on the VNC Server icon:
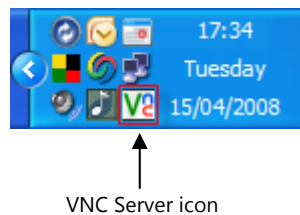
VNC Server icon

This displays the VNC Server Status dialog:
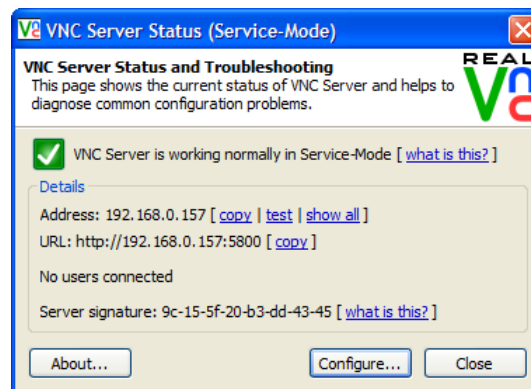
To configure VNC Server for maximum security

Authentication and *Encryption* are the most important factors when configuring VNC Server for maximum security.

1. On the VNC Server Status dialog, click **Configure**:

   This displays the VNC Server Properties dialog:
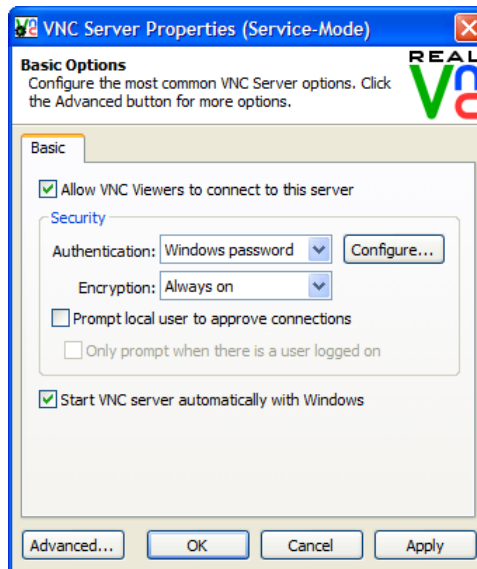
The first time that you start VNC Server, the *VNC Server Properties* dialog will display in *basic* mode with the most frequently used configuration options. In order to display all of the available configuration options, click the **Advanced** button. (To switch back to basic mode, click the **Basic** button at any time).
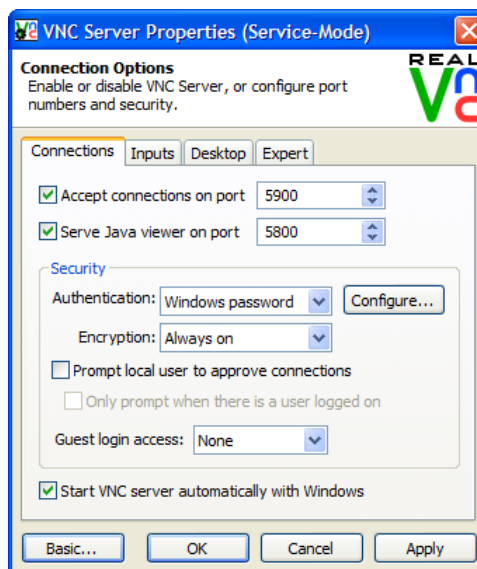
<div style="border:2px solid red; text-align:center; font-weight:bold;">
THIS GUIDE WILL ASSUME THAT YOU ARE WORKING IN ADVANCED MODE.
</div>

By default, the VNC Server Properties dialog opens on to the **Connection Options** tab which gives you control of all of the connection options for your VNC Server.

2. For maximum security, in the **Security** area, your settings should match those below:
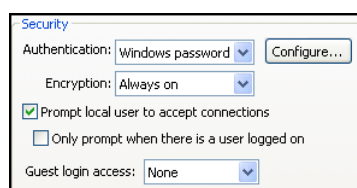
Security Option	Setting
Authentication	Windows Password
Encryption	Always on
Prompt local user to accept connections	Yes
Only prompt where there is a user logged on	-
Guest login access	None

NB: You should not need to alter the VNC Port numbers within VNC Server, however if you do, all VNC Viewers must specify the new port number when attempting to connect to the VNC Server. For more details on this, and other advanced connection options, please refer to the Connection Settings section.

To configure VNC Server for maximum speed

The server's speed response is affected by three factors:

1. Encryption – Data encryption imposes small performance overheads. Where security is not a priority or the threat of data interception is low, the **Encryption** option should be set to **Prefer Off**:
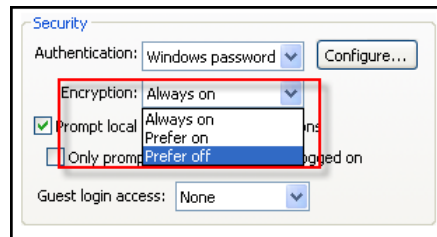
2. Ports – Combining the *Accept connections on port* and *Serve Java viewer on port* to use the same number can lengthen the initial connection time by up to two seconds. To minimise the initial delay when connecting, ensure that these options are set to use different port numbers:
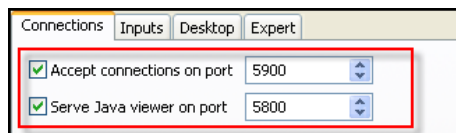
3. Desktop Optimisation – By optimising desktop effects, you can increase the response time. All three options should be enabled to maximise response time.

On the VNC Server Properties dialog, click the **Desktop** tab to display the **Optimisation** area:
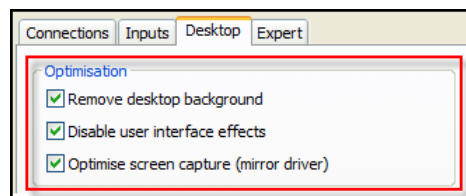
Ensure that the above options are checked.

Using the VNC Service

By default, VNC Server is configured to start automatically when Windows starts. You can also start and stop the service manually.

Starting the service

1. Click the Windows **Start** button, then point to **Programs** (or All Programs), then point to **RealVNC → VNC Server**:
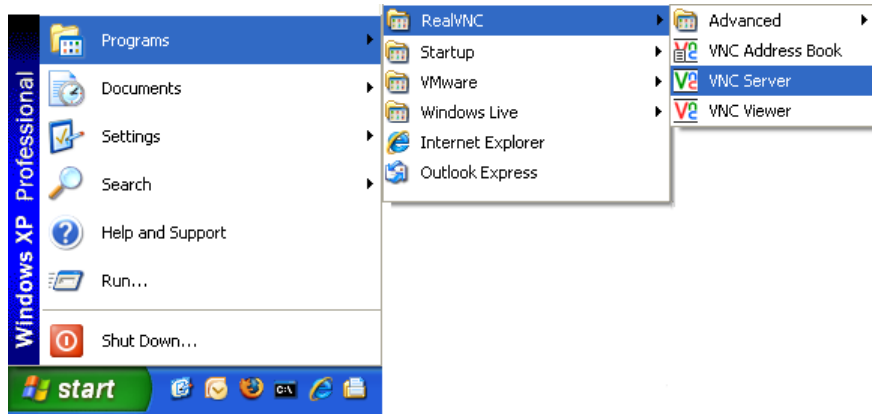
    VNC Server will start.

Closing the service

1. Right-click on the VNC Server icon in the Windows Task Tray, and select **Stop VNC Server**:
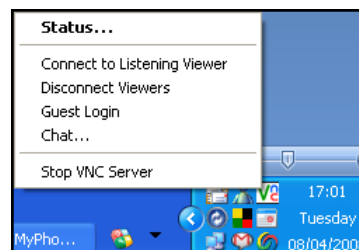
    A confirmation dialog will be displayed:
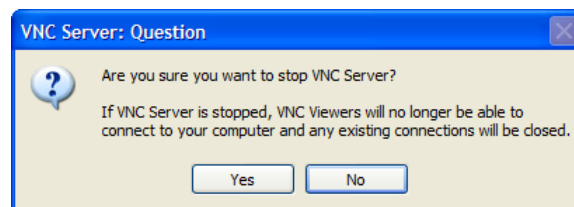
2. Click **Yes** to close the VNC Server.

Using the VNC Server taskbar tray icon

When VNC Server is running, it uses minimal system resources and will only visible as an icon in the windows task tray:
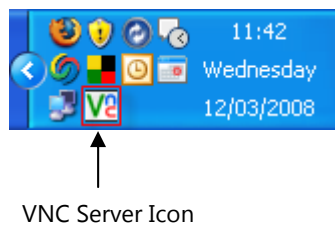
VNC Server Icon

The icon displays the current status of the VNC Server:

Icon	VNC Status
	The VNC Server is running: no active viewers connected.
	The VNC Server is running: active viewers connected.
	The VNC Server is disabled
	There is a problem with the VNC Server

- Double-click the VNC Server icon to display the VNC Service Status dialog.
- Right-click on the VNC Server icon to display a context menu; the following table describes the options:

| Context Menu Option	Description
Status	Displays the VNC Server Status Dialog
Connect to Listening Viewer	Connects to the VNC Listening Viewer
Disconnect Viewers	Ends all current viewers' connections to your VNC Server
Guest Login	If you have enabled this feature, viewers can connect without supplying security credentials. Click to turn on/off.
Chat	Opens a window to enable chat with connected viewers
Send Files to Viewers	If connected to a viewer, you are able to send a file to the viewer's computer. (*This option is unavailable in service-mode; instead, you can send files to viewers by copying them to the clipboard*).
Fetch Files from Viewers	If connected to a viewer, you are able to fetch a file from the viewer's computer. (*This option is unavailable in service-mode; instead, files sent by viewers are put on the clipboard and can be pasted*).
Stop VNC Server	Closes the VNC Server and disconnects any connected viewers.

Advanced Configuration & Reference

The following sections provide full reference information for all of the advanced configuration options available in VNC Server.

Connection Settings

Ports
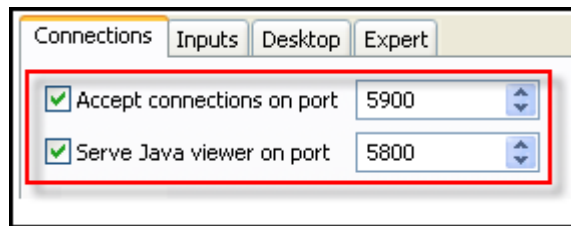
You should not need to alter the VNC Port numbers within VNC Server, however if you do, all Viewers must specify the new port number when attempting to connect to the VNC Server.

Accept connections on port

This option indicates through which main connection port viewer clients will be served. VNC Viewers expect the standard setting of port 5900. However, if this port clashes with another local network service, then it can be changed to use any other vacant port number. If you do alter the port number, you must specify the new port number when connecting via the VNC Viewer.

To disable any VNC Viewer connections, uncheck this option.

Serve Java Viewer on port

This option specifies the port through which VNC Server will provide the Java viewer applet, when requested, to java enabled web browsers. By default, the Java Viewer port will be 100 lower than the connections port and will change accordingly whenever the main connections port is altered. You may wish to have the Java viewer served on the same port as the connections port in order to simplify firewall configuration.

You can disable the Java Viewer by un-ticking the *Serve Java Viewer on Port* check box.

For further information about ports, refer to the Ports section in the Appendix

Authentication Options

To display:

- Double-click the VNC Server icon in the Windows task tray, and click **Configure**. This displays the VNC Server Properties dialog, ensure that the **Connections** tab is selected. Authentication options are displayed in the **Security** area:
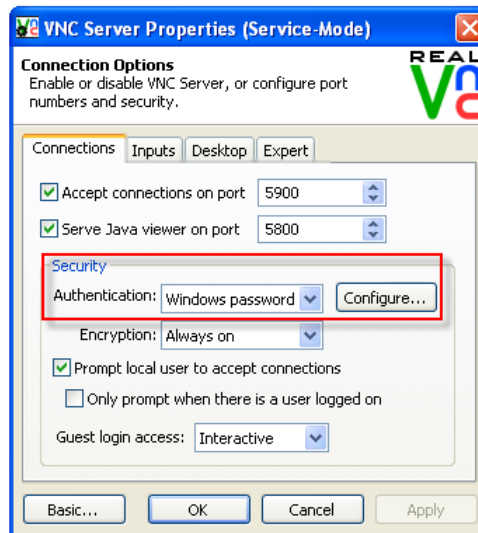
There are four authentication options available from the **Authentication** drop-down list:

- VNC Password
- Windows Password
- Single Sign-on
- None

The table below summarises the authentication options available.

Authentication Option	Description
VNC Password	Requires any Viewer application to supply a valid password before access to the Server system is allowed.
Windows Password	Links to the internal Windows security system within Windows NT, 2003, XP, and Vista. This enables you to grant different permissions for different types of users, e.g. administrators, guests, users, using Windows User Configurations.
Single sign-on	Allows you to connect using your windows password and username. You will not be prompted for a username or password when you try to connect. Both the Server and Viewer must have this option enabled.
None	Allows Viewer applications to connect to the VNC Server without supplying a username or password. This is useful when the VNC Server is operating within a completely secure environment such as a Local Area Network or Virtual Private Network. **NB: Do not use unless the host network is known to be completely secure**

VNC Password usage

Using the VNC Password for authentication requires any Viewer application to supply a valid password before access to the Server system is allowed. You can create up to three passwords, each up to 255 characters in length for a standard, admin and view-only user.

To create a standard VNC Password:

- Click **Configure**. This displays the following dialog:
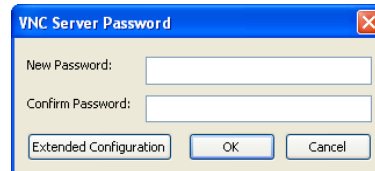
- In the **New Password** text box, enter a password, enter again in the Confirm Password text box, and then click **OK**.

To create additional passwords:

- Click **Configure**, and then click **Extended Configuration**. This displays the following:
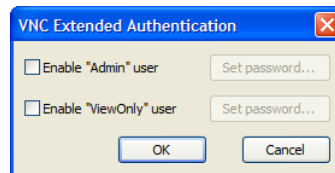
- Select the users you want to enable, and the click the corresponding **Set Password** buttons to enter passwords for each user.

User descriptions

User Type	Description
Admin	Users have full access (keyboard, mouse, clipboard), and the local user is not prompted to approve the connection.
ViewOnly	Users have permission to view the desktop, but cannot interact with it. Mouse and keyboard input, and access to the remote clipboard is disabled.

Windows Password usage

Using the Windows Password for authentication takes advantage of the internal Windows security system within Windows NT, 2003, XP, Vista and 2008. This enables you to grant different permissions/user rights for different types of users, e.g. administrators, guests, users, using Windows User Configurations. There are two steps required to set up VNC server for Windows Password authentication:

1. On the **Authentication** drop-down list, select **Windows Password**.
2. Click **Configure**; this displays the Permissions for VNC Server dialog which lists the available user rights:
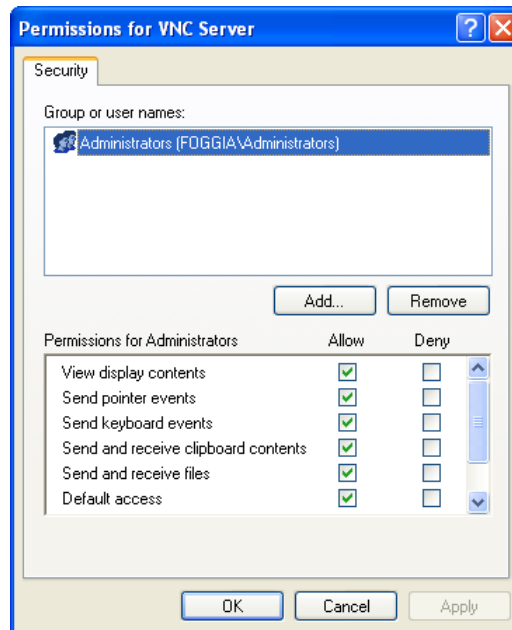
User Right	Description
View display contents	The viewer can view the contents of the VNC Server desktop.(recommended)
Send pointer events	The viewer can interact with the VNC Server using the mouse.
Send keyboard events	The viewer can interact with the VNC Server using the keyboard
Send and receive clipboard contents	Clipboard contents are synchronised between the VNC Viewer and the VNC Server.
Send and receive files	File transfer is available between the VNC Viewer and the VNC Server.
Default access	Allows all of the above permissions, plus new user rights as they become available, they are by default granted to users.
Connect without accept/reject prompt	The viewer can connect without the VNC Server user having to manually accept the connection.
Full Access	Viewers have all available user rights. When new user rights become available, Viewers, (with full access enabled) will automatically have access to them.

The default user rights granted to users and groups are as follows:

Default User Rights	User/Groups
Full Access	Members of the local Administrators group Members of the local or domain VNC Admins group, if available.
Default Access	Members of the local or domain VNC user group, if available.
View Display Contents	Members of the local or domain VNC View-only group, if available.

NB: The user rights enabled for users and groups using Windows Password authentication, will always take priority over any other authentication settings.

Single Sign-on

Like Windows Password usage, *Single Sign-on* allows you to use the Windows username and password for authentication and takes advantage of the internal Windows security system within Windows NT, 2003, XP, Vista and 2008. The only difference between Single sign-on and Windows Password usage, is that for Single Sign-on you will not be prompted to enter a username or password. All other user rights settings are identical to Windows Password usage.

No authentication

If selected, this option allows Viewer applications to connect to the VNC Server without supplying a username or password. This option is useful when the VNC Server is operating within a completely secure environment such as a Local Area Network or Virtual Private Network, to remove the requirement for authentication.

NB: Do not use unless the host network is known to be completely secure.

NB: Encryption can be used even if *No authentication* is selected.

Encryption Options

There are 3 encryption options available for VNC Server:
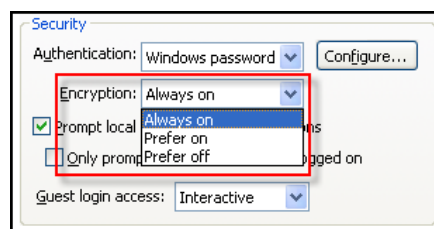
Each option determines how encryption will be applied to user connections:

Encryption Option	Description
Always on	Viewer connections will always be encrypted.
Prefer On	Viewer connections will be encrypted unless a VNC Viewer has encryption set to Prefer Off, in which case encryption would be off.
Prefer Off	Viewer connections will not be encrypted unless a VNC Viewer has encryption set to Prefer On or Always on, in which case encryption would be on.

Other Security Settings

In addition to encryption and authentication options, there are three other settings available on the Connections page that effect security:
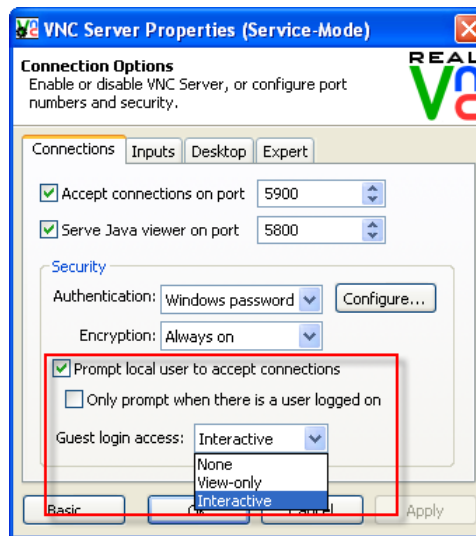
The following table describes these options:

Option	Description
Prompt local user to accept connections	A confirmation dialog is displayed on the VNC Server system indicating that a Viewer is attempting to connect. The dialog will display the Viewer's IP address and their user name. If no response is given by the Server user within 10 seconds, the Viewer request is rejected.
Only prompt where there is a user logged on	If no Server user is logged on, Viewers will be able to connect (subject to their established user rights).
Guest login access	Server users can use *Guest login* to temporary allow access to the server system. It is accessed from the right-click context menu on the VNC Server icon in the task tray. • *None* disables the Guest Login access from the task tray icon. • *View-only* enables the Viewer to connect to the Server with View Only user rights. • *Interactive* enables the Viewer to connect to the Server with interactive user rights.

Input Options

The *Inputs* tab on the VNC Server Properties dialog allows you to determine the level of control that incoming VNC Viewers can have over the VNC Server system:
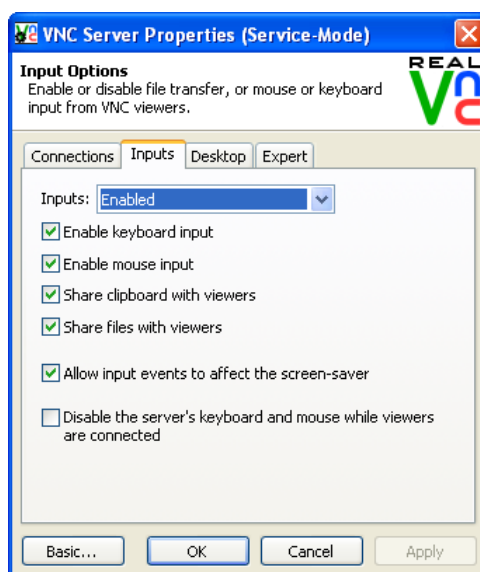
- To allow all inputs (keyboard, pointer, clipboard, file sharing), on the **Inputs** drop-down list, select **Enabled**.

- To disable all inputs so that the Viewer has View Only, on the **Inputs** drop-down list, select **Disabled**.

- To choose a custom level, on the **Inputs** drop-down list select, **Custom**, and then select the options you require by clicking the appropriate check box.

The following table describes the different Input options:

Input Option	Description
Enable keyboard input	Viewer can interact with the Server using their keyboard.
Enable mouse input	Viewer can interact with the Server using their mouse.
Share clipboard with viewers	Server clipboard is shared with the Viewer.
Share files with viewers	Files can be transferred between Viewer and Server, and vice versa.
Allow input events to affect the screen-saver	Incoming viewer inputs will interrupt the Server screensaver (if present).
Disable the server's keyboard and mouse while viewers are connected.	When Viewers are connected, local input to the Server is disabled.

Desktop Options

The *Desktop* tab on the VNC Server Properties dialog allows you to fine tune performance by reducing unnecessary VNC Server desktop effects from being transmitted to the Viewer. It also allows you to determine how the VNC Server system should be left after Viewer access:
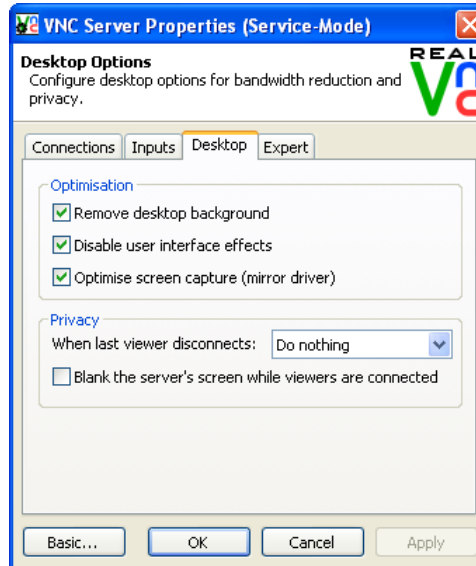
Desktop Options	Description
Optimisation	
Remove desktop background	If enabled, any wallpaper image used on the VNC Server system will be removed and replaced with a plain background when a VNC Viewer is connected. This option will also attempt to disable Windows Active Desktop if used. This can help to reduce transmitted data and improve overall performance.
Disable user interface options	If enabled, any visual user effects such as animated drop-down menus will be disabled when a VNC Viewer is connected. This can help to reduce transmitted data and improve overall performance.
Optimise Screen capture (mirror driver)	If enabled, this gives the best possible visual performance. **NB**: The mirror driver is only available in *Service* mode.
Privacy	
When last viewer disconnects	You can choose in what state to leave the server when a viewer disconnects. The options are *Do nothing*, *Lock workstation*, or *Log Off*.
Blank the server's screen while viewers are connected.	If enabled, the server's screen will be blanked when viewers are connected to the server.

VNC Chat

VNC Enterprise Edition 4.4 includes a simple "chat" application. This enables the VNC Viewer user to communicate with the VNC Server user and vice versa.

To start a chat

3. Ensure that you are connected to a VNC Server, and on the VNC Server window, in the Windows task tray, right click the VNC Server icon, and select **Chat**:
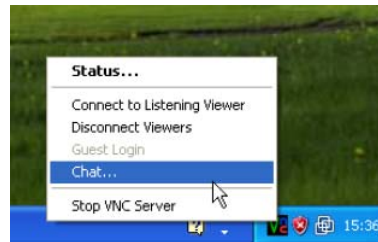
4. This displays the *VNC: Chat Messages* dialog:

Enter text here
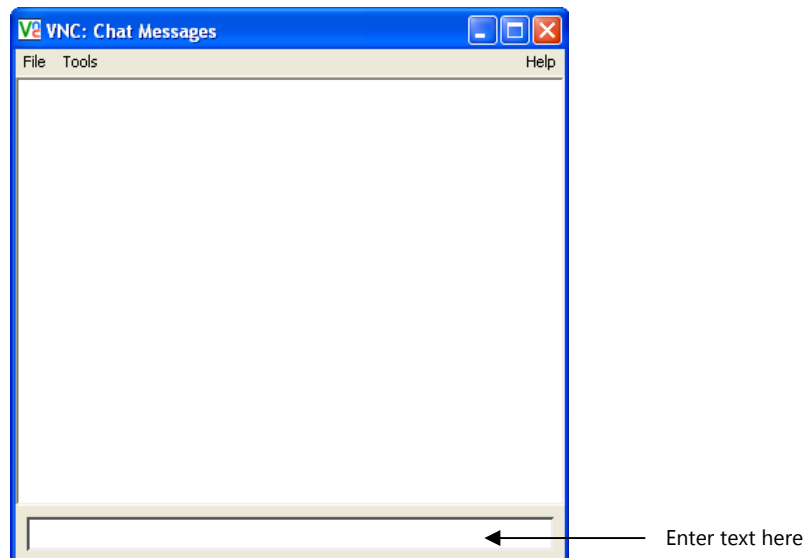
To enter a message, simply type in the text field, and then press the **Enter** key to send the message. The example below shows a message sent from VNC Viewer user (user) to the VNC Server user (Admin Local):
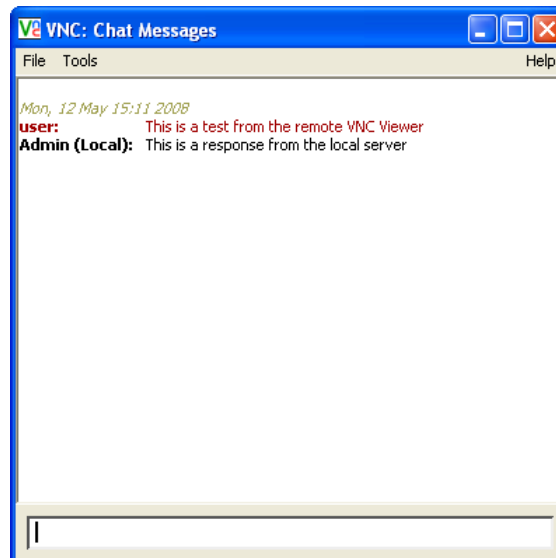
VNC Chat options

By default, the VNC Chat application is set to save all chat messages for 90 days. To change these options:

5.   On the **Tools** menu, select **Options**. This displays the *Options* dialog:
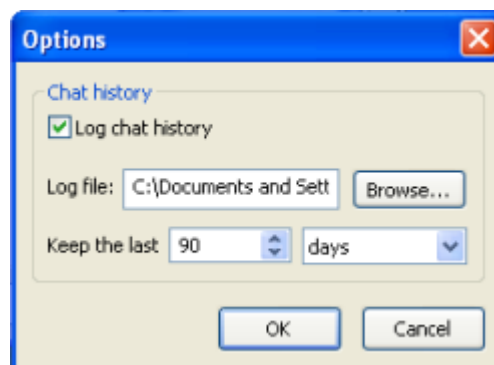
6.   If you don't want to keep a log of your chat history, uncheck the **Log chat history** option.

7.   By default, the Log file is stored in:

    `C:\Documents and Settings\username\Application Data\RealVNC`

    To change this, click the **Browse** button, and navigate to the folder where you would like to store the log file.

8.   By default the last 90 days of chat messages will be logged. However instead of storing by a number of days, you can choose to store by number of messages. to change this:

   • On the **Keep the last** box, enter the number of days or messages that you would like to keep.

   • On the **days** drop-down box, choose between *days* or *messages*

Copying messages from chats

You can copy Chat messages to any text based application.

To do this:

- Simply select the messages that you want copy, then press Ctrl+C, and then paste into your chosen text based application, such as Microsoft Word, WordPad, or Notepad.

Listening Viewer (Server initiated connection)

In certain circumstances it can be preferable for the VNC Server to initiate connections to one or more viewers, rather than the other way round. For instance:

- Firewalls can often cause problems for incoming connections to server systems. When the server initiates the connection to a viewer, this problem is overcome. The firewall must, however, allow outgoing connections through port 5500. Also, if the viewer system is behind its own firewall, then that must allow incoming connections, also at port 5500.

- Where VNC is used in a classroom or presentation environment, the tutor/presenter can make his server initiate connections to each of the viewer systems. In this way greater overall control is retained and this method obviates the need to provide server connection information to each user.

To create a listening viewer connection

On the VNC Viewer system:

1. Start the listening viewer by clicking the Windows **Start** button, then point to **Programs** (or All Programs), then point to **RealVNC ➔ Advanced ➔ VNC Viewer (Listening Mode)**.

On the VNC Server system:

1. Right click on the VNC icon in the windows task tray, and select **Connect to Listening Viewer**. This displays the *VNC Server: Connect to Listening Viewer* dialog:
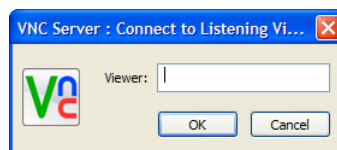
2. Enter the IP address of the viewer system and click OK. No username or passwords are required.

Providing the correct address is entered and there are no firewall issues with the viewer system, the VNC Viewer will display the server's screen as if it had initiated the connection in the usual manner.

To end a listening viewer connection

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

- From the VNC Viewer: Close the viewer window.
- From the VNC Server: Right-click on the VNC Server icon in the windows task tray and select the **Disconnect Viewers**.

Technical Support

If you are have a problem, please refer to our online FAQ page on the RealVNC website. If you still cannot find a solution, then please don't hesitate to contact us for further assistance using the product support request page

Support request

This section allows you to send queries directly to a VNC support representative:

www.realvnc.com/support.html

Please include as much information as possible about 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 your customer number and registered email address and the version of VNC Server and VNC Viewer that you are using, and operating system you are running at both ends of the connection.

Acknowledgements

VNC Enterprise Edition 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/enterprise/4.4/acknowledgements.html

Appendix

Ports

What is a port?

Not to be confused with a physical port (such as a USB, or printer port) to which you connect devices, a Port in this context could be more accurately described as a 'service contact point'. It provides an indication of where to locate an appropriate known service that can deal with the kind of data being transmitted.

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 is 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.

You should not normally need to change the VNC port number within VNC Server 4, however,
if you do, then all viewers must declare the new port number when connecting to the the server system.
For instance, if the port number was changed to 5950, then to reach a server at IP address 192.168.0.2,
the VNC Viewer user would need to enter:

```
192.168.0.2::5950
```

(note the double colons)

Port numbers can range from 0 to 65,535 and are generally divided into three ranges:

- 0 to 1023 are well known ports

- 1024 to 49151 are registered ports

- 49152 to 65535 are dynamic and/or private ports

A list of valid port numbers and their uses is maintained by the Internet Assigned Numbers Authority and can be viewed at http://www.iana.org/assignments/port-numbers. Port 5900 is officially registered with IANA for VNC use.

Firewalls

Dealing with firewalls

A common cause of VNC operational failures are related to firewalls. One of the key functions of a network firewall is to block the use of most port numbers by incoming network traffic in order to prevent access by unauthorised or malicious users. Therefore, unless an exception is made for the specific ports used by VNC, any attempt to connect to a VNC Server situated behind a firewall will be denied.

There are a number of options available to you in these situations:

- Adjust the firewall rules to allow incoming traffic via the ports required by VNC, i.e. Port 5900 and port 5800.
  NB: Firewall rule changes should be carried out only by an experienced operator. Incorrect configuration could leave a network open to attack. The exact details for changing rules alter between differing firewall types and are beyond the scope of this guide.

- Place the VNC Server system outside the firewall and use its security to allow only authorised users.
  NB: When placing the VNC Server externally to a firewall, i.e. with open access to an outer network, such as the Internet, it is vital that full security features are employed, both within VNC Server 4 and also for the operating system upon which the server is running. See the Connection Settings section more details.

- Set VNC viewers to 'listen' and initiate connections from the VNC Server 4.
  This removes the need to make the server accessible from outside the firewall. See Listening viewer for details.

- Use Windows Firewall (Windows XP Service-Pack 2 and newer).
  Recent versions of Windows XP include a built-in firewall. From Service Pack 2 onwards, the firewall can be easily configured to allow particular applications to open whichever ports they require. By adding an 'Application Exception' to the Windows Firewall for the VNC Server, both User- and Service- mode servers can be made accessible remotely without the need for port numbers to be specified explicitly. The VNC server is able to detect Windows Firewall and configure it automatically when the VNC Server Properties dialog is dismissed.

IP Addresses

What is an IP address?

An IP address is a unique address 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. 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. However, two factors have proved this to be wrong:

1. The proliferation and expansion of the Internet,
2. The 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. 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. However, when company xyz 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 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, 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.

Windows Version Support

Most releases of Windows are supported by VNC Server 4. Some versions, however, lack certain functionality or cause known problems.

Older Windows versions

VNC Server 4 is not designed to operate with older versions of Windows including 3.1, 3.11, 95, NT 3.1 or NT 3.51.

Windows 98 / Windows Me

Under Windows 98 and Windows ME it is not possible for the VNC settings (including the server's password) to be properly secured in the registry - this is an intrinsic limitation of these platforms. NT Logon authentication is not supported on these platforms. Public-key based Server authentication and 128-bit session encryption are supported on these platforms, with the caveat that server private keys cannot be secured in the registry, since they do not support registry security.

Windows NT 4.0

VNC Server 4 will not run in Service Mode unless Windows NT Service Pack 3 or later has been installed. VNC Server 4 can be operated in User Mode. Note that Windows NT 4.0 does not support the NT Logon authentication configuration dialog at this time.

Windows XP, Vista and 2008

VNC Server 4 is fully compatible with Windows XP, Vista and 2008.