

VNC® Enterprise Edition

User Guide

Version 4.5

April 2010

Trademarks

VNC is a registered trademark of RealVNC Ltd. in the U.S. and in other countries. Other trademarks are the property of their respective owners.

Copyright

Copyright © RealVNC Limited, 2010. 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

All information contained in this document is provided in commercial confidence for the sole purpose of use by an authorized user in conjunction with RealVNC 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.

Contact

RealVNC Limited
Betjeman House
104 Hills Road
Cambridge
CB2 1LQ
United Kingdom
www.realvnc.com

Contents

| | | |
|-------------------|--|-----------|
| | About This Guide | 7 |
| Chapter 1: | Introducing VNC Enterprise Edition | 9 |
| | What is VNC Enterprise Edition? | 10 |
| | Getting VNC Enterprise Edition ready to use | 10 |
| | VNC Enterprise Edition 4.5 connectivity | 12 |
| | What to read next | 13 |
| Chapter 2: | Getting Started: Connecting A Client To A Host Computer | 15 |
| | Step 1: Ensure VNC Server is running on the host computer | 16 |
| | Step 2: Start VNC Viewer on the client computer | 17 |
| | Step 3: Identify VNC Server on the host computer | 17 |
| | Step 4: Select an encryption option | 19 |
| | Step 5: Connect and authenticate to VNC Server | 19 |
| | Troubleshooting connection | 21 |
| Chapter 3: | Using VNC Viewer | 29 |
| | Starting VNC Viewer | 30 |
| | Configuring VNC Viewer before you connect | 31 |
| | Connecting to a host computer | 35 |
| | Connected: The VNC Viewer experience | 36 |
| | Using the VNC Viewer toolbar | 38 |
| | Using the VNC Viewer shortcut menu | 39 |
| | Using the VNC Viewer Properties dialog | 41 |
| | Managing the current connection | 42 |
| | Changing the appearance and behavior of VNC Viewer | 43 |
| | Restricting access to functionality | 45 |

| | | |
|--------------------|--|------------|
| Chapter 4: | Connecting From A Web Browser | 49 |
| | Connecting to a host computer | 50 |
| | Connected: The VNC Viewer for Java experience | 54 |
| | Working with VNC Viewer for Java | 55 |
| Chapter 5: | Exchanging Information | 59 |
| | Printing host computer files to a local printer | 60 |
| | Transferring files between client and host computers | 62 |
| | Copying and pasting text between client and host computers | 66 |
| | Communicating securely using VNC Chat | 67 |
| Chapter 6: | Setting Up VNC Server | 71 |
| | Starting VNC Server | 72 |
| | Running multiple instances of VNC Server | 76 |
| | Working with VNC Server | 79 |
| | Configuring network communications | 86 |
| | Preventing connections to VNC Server | 88 |
| | Restricting functionality for connected users | 90 |
| | Stopping VNC Server | 92 |
| Chapter 7: | Security | 93 |
| | Authenticating connections to VNC Server | 94 |
| | Relaxing the authentication rules | 99 |
| | Bypassing the authentication rules | 102 |
| | Relaxing the encryption rules | 105 |
| | Preventing particular connections to VNC Server | 106 |
| | Restricting functionality for particular connected users | 110 |
| | Uniquely identifying VNC Server | 114 |
| | Upholding privacy | 115 |
| Appendix A: | Saving Connections | 117 |
| | Saving connections to VNC Address Book | 118 |

| | |
|---|-----|
| Using VNC Address Book to connect | 123 |
| Managing connections using VNC Address Book | 124 |
| Saving connections to desktop icons | 127 |

About This Guide

This User Guide explains how to use *VNC Enterprise Edition 4.5* to connect two computers over a TCP/IP network and control one from the other. The two computers can be running any supported operating system.

Note: All the information in this User Guide also applies to *VNC Personal Edition 4.5* with the exception of sections on platform-native authentication, and to *VNC Viewer Plus 1.0* for connections made to *VNC Server*.

Intended audience

There is no such thing as a typical *VNC Enterprise Edition* user. This User Guide therefore has more than one audience in mind:

- Chapter 1 is a general introduction to *VNC Enterprise Edition*, intended for everybody.
- Chapter 2 through 5 are intended for users who want to connect to and control a remote computer.
- Chapters 6 and 7 are intended for users who want to set up the computer to be controlled.

This User Guide is intended to be operating system-agnostic, as far as possible. Information related to specific operating systems is clearly marked.

Conventions

Most dialogs and other artifacts are identified by the operating system under which graphics were captured. The default for generic dialogs is Windows XP. These may appear different under UNIX or Linux and Mac OS X, or versions of Windows with different themes, but the principle is the same. Note that error messages and partial dialogs are not identified.

Services

You can e-mail RealVNC Support if you have a full or trial license to use *VNC Enterprise Edition*. At the time of publication, this service is available from www.realvnc.com/support/index.html.

Related information

Navigate to www.realvnc.com for:

- Supported platforms, operating systems, and system requirements.
- Instructions on how to install, unlock, and remove *VNC Enterprise Edition*, and getting a trial license key.
- Release Notes and FAQs.
- Downloads of related programs.
- Information relating to earlier versions of *VNC Enterprise Edition*.

About This Guide

- Information relating to other RealVNC products and solutions.

Note: Under Windows, once *VNC Enterprise Edition* is installed, you can go straight to the *VNC Enterprise Edition* home page from the **Start** menu. Select **RealVNC > Documentation > VNC Enterprise Edition on the web**.

1

Introducing VNC Enterprise Edition

This chapter introduces *VNC Enterprise Edition*: what it is, how it works, and how it can help you.

It explains what you need to do to get *VNC Enterprise Edition* ready to use in your environment and suggests, for users with different requirements, what chapters of this User Guide to read next.

Note: All the information in this User Guide also applies to *VNC Personal Edition* with the exception of sections on platform-native authentication, and to *VNC Viewer Plus* for connections made to *VNC Server*.

Contents

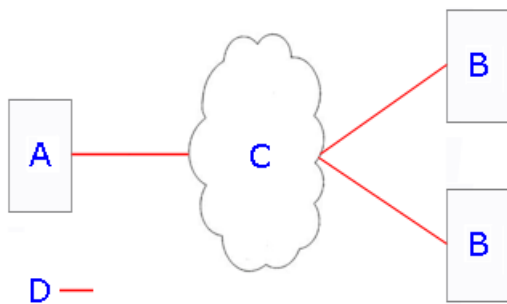
| | |
|---|----|
| What is VNC Enterprise Edition? | 10 |
| Getting VNC Enterprise Edition ready to use | 10 |
| VNC Enterprise Edition 4.5 connectivity | 12 |
| What to read next | 13 |

What is VNC Enterprise Edition?

VNC Enterprise Edition connects two computers together over a network and enables you to take control of one (the *host computer*) from the other (a *client computer*) irrespective of where the two are in the world, or incompatibilities they may have in platform, architecture, or operating system.

VNC Enterprise Edition consists of two separate programs, *VNC Server* and *VNC Viewer*. You install and run *VNC Server* on the host computer; that is, the computer to be controlled. You run *VNC Viewer* on the client computer, use it to establish an encrypted, authenticated connection to the host computer and, when *VNC Viewer* displays the host's desktop in a new window, take control of it using the client's keyboard and mouse. You can run applications, change settings, and access data on the host computer exactly as you would be permitted to do were you sitting in front of it.

Note: Other users can connect to the host computer at the same time as you. You may be sharing control.



A. Host computer running *VNC Server*. **B.** Client computers running *VNC Viewer*, each connected to *VNC Server*, and displaying the host computer's desktop. **C.** A network, for example a Local Area Network or the Internet. **D.** Secure (authenticated and encrypted) connections.

VNC Enterprise Edition solves different problems for users with different requirements, from the family member troubleshooting computer problems over the Internet to the system administrator configuring devices remotely for the enterprise environment. To find out how to get the information you need from this User Guide, see *What to read next* on page 13.

Getting VNC Enterprise Edition ready to use

Before you can establish a connection, certain operations must be performed on both host and client computers.

This section addresses the client computer user and assumes the same person is able (that is, is physically present and has sufficient privileges) to configure the host computer as well. If not, contact a system administrator or a host computer user.

Note: Some operations need only be performed once. Others must be performed before each connection.

Host computer

1. Ensure the host computer is turned on, has a functioning operating system, and is connected to a network to which the client computer can also connect. For example:
 - A private network such as a LAN or VPN, if both computers are co-located at home or in a typical small office environment.
 - A public network such as the Internet for most other kinds of connection, and especially those made from an Internet café, using a public Wi-Fi hotspot, or over a mobile (cellular) data network (3G/GPRS/EDGE).
2. Install and license the *VNC Server* component of *VNC Enterprise Edition*. You will need to be logged on as a user with administrative privileges. For detailed instructions, navigate to the installation and licensing documentation appropriate to the platform of the host computer at <http://www.realvnc.com/products/enterprise/4.5>.
3. If you are connecting over the Internet, it is very likely the host computer will be protected by at least one firewall. If so, each must be configured to allow network communications through to the port on which *VNC Server* is listening, which is 5900 by default. See *Allowing network communications through a firewall* on page 26 for more information.
4. If you are connecting over the Internet, it is very likely the host computer will be protected by at least one router. If so, each must be configured to forward network communications through to the port on which *VNC Server* is listening, which is 5900 by default. See *Configuring a router to forward network communications* on page 23.
5. Make sure *VNC Server* is running on the host computer and that it can accept incoming connections. See *Step 1: Ensure VNC Server is running on the host computer* on page 16 for more information.
6. Find out the network address of *VNC Server*. If you are connecting:
 - Over a LAN or VPN, this must be a private address, which is that of the host computer itself. See *Connecting within a private network* on page 21 for more information.
 - Over the Internet, this must be a public address, which is that of a router or similar device. See *Connecting over the Internet* on page 22 for more information.
7. Find out the user name and password of a user with administrative privileges on the host computer or, if no such credentials exist, change the default authentication mechanism. See *Authenticating connections to VNC Server* on page 94 for more information.

Note: If you cannot perform these operations and a host computer user is present, you may be able to set up a *reverse connection*. See *Establishing a reverse connection* on page 104 for more information.

Client computer

1. Ensure the client computer is turned on, has a functioning operating system, and is connected to the same network as the host computer.
2. Obtain *VNC Viewer*. You can either:
 - Install the fully-featured *VNC Viewer* component of *VNC Enterprise Edition*.
 - Download standalone *VNC Viewer* from the RealVNC web site. This is useful if you do not want, or have sufficient privileges, to install software. For information on limitations in this mode, see *Connecting from standalone VNC Viewer* on page 13.

For detailed instructions, navigate to the installation documentation appropriate to the platform of the client computer at <http://www.realvnc.com/products/enterprise/4.5>. Note you do not need a license to use *VNC Viewer*.

3. Run *VNC Viewer* and connect. Carry on from *Chapter 2, Getting Started: Connecting A Client To A Host Computer* on page 15.

Note: If you do not want to use *VNC Viewer*, you can simply connect from any Java-enabled web browser. However, there are considerable limitations in this mode. See *Connecting from a web browser* on page 13 for more information.

VNC Enterprise Edition 4.5 connectivity

Unless stated, this User Guide assumes you are connecting from a client computer running fully-featured *VNC Viewer 4.5* to a host computer running *VNC Server 4.5*. However, you can also:

- Use *VNC Viewer 4.5* to connect to:
 - A version of *VNC Server* prior to 4.5.
 - A computer running *VNC Personal Edition* or *VNC Free Edition*.
 - A Mac OS X computer with Screen Sharing or Remote Management built-in and enabled (turn on **VNC viewers may control screen with password**, and set a password).
 - A VNC-compatible Server product from a third party.

Note that not all the functionality of *VNC Enterprise Edition 4.5* is available in each circumstance.

- Connect to *VNC Server 4.5* from:
 - A version of fully-featured *VNC Viewer* prior to 4.5.
 - Standalone *VNC Viewer*.
 - A Java-enabled web browser.

Note that not all the functionality of *VNC Enterprise Edition 4.5* is available in each circumstance. See the sections below for more information.

Connecting from an earlier version of VNC Viewer

You can connect to *VNC Server 4.5* from a version of *VNC Viewer* prior to 4.5, but note that features new to this release will not be available. In particular, you cannot:

- Print host computer files.
- Copy and paste text containing special characters between applications running on the client and host computers. You can only copy and paste characters from the Latin-1 (ISO 8859-1) character set.
- Chat with other connected users, or with a host computer user, on computers running UNIX or Linux or Mac OS X.

Note: You may not be able to connect to *VNC Server* at all if your version of *VNC Viewer* does not support encryption and authentication. For more information, see the RealVNC web site.

Connecting from standalone VNC Viewer

You can connect to *VNC Server 4.5* from standalone *VNC Viewer*. This application is freely available to download and run for any supported platform from the RealVNC web site. Note if you use standalone *VNC Viewer*, you cannot:

- Save connections to *VNC Address Book*. You can still save connections to desktop icons.
- Under Windows, print to a local printer if the host computer is running UNIX or Linux or Mac OS X. You can only print if the host computer is also running Windows.

Connecting from a web browser

You can connect to *VNC Server 4.5* from a Java-enabled web browser. For more information, see *Chapter 4, Connecting From A Web Browser* on page 49. Note if you do this, you cannot:

- Print host computer files.
- Exchange files with the host computer.
- Chat with other connected users, or with a host computer user.
- Save connections to *VNC Address Book* or to desktop icons.
- Scale the host computer's desktop.

What to read next

VNC Enterprise Edition can be used in many different ways to solve many different kinds of problem. There is no such thing as a typical *VNC Enterprise Edition* user.

For example, you may be sitting in front of a host computer and need to know how to set up *VNC Server* for multiple incoming connections. Or you may be sitting in front of a client computer and want to know how to use *VNC Viewer* to control a remote host. There may or may not be a host computer user for you to communicate with, or you may be sharing the host computer's desktop—and therefore control—with other users. You may be connecting within a corporate network, in which case a system administrator might be available to help with connection issues. Or you may be helping friends or family over the Internet, and have to negotiate firewalls and routers on your own.

VNC Enterprise Edition is designed to be as useful out-of-the-box to as many people as possible. However, there is virtually no limit to the ways in which it can be configured to suit your requirements and environment. Some chapters in this manual are targeted at more expert users, likely to require the power of changing options – system administrators setting up *VNC Enterprise Edition* for virtualization or remote configuration, for example. Other chapters, especially the first two, should be useful for all users.

- To walk through making your first connection from a client computer running *VNC Viewer* to a host computer running *VNC Server*, see *Chapter 2, Getting Started: Connecting A Client To A Host Computer* on page 15.
- To learn how to use features of *VNC Viewer* to enhance your experience of controlling a host computer, read *Chapter 3, Using VNC Viewer* on page 29.
- If you want to control a host computer from a web browser instead of *VNC Viewer*, read *Chapter 4, Connecting From A Web Browser* on page 49.

Chapter 1: Introducing VNC Enterprise Edition

- To see how to exchange information between client and host computers, read *Chapter 5, Exchanging Information* on page 59.
- To learn how to configure *VNC Server* on the host computer, and for advanced topics such as running multiple instances of *VNC Server*, see *Chapter 6, Setting Up VNC Server* on page 71.
- By default, *VNC Enterprise Edition* establishes authenticated, encrypted connections. To learn more about security, and how to relax the rules if you consider it safe to do so, read *Chapter 7, Security* on page 93.

2

Getting Started: Connecting A Client To A Host Computer

This chapter aims to help the majority of users get started making their first connection from a client computer running *VNC Viewer* to a host computer running *VNC Server*.

Connecting is usually a straightforward process but because computer networks must be secure problems can occasionally occur. This chapter offers help for the most common connection issues but it may also be necessary to consult the RealVNC web site, or contact Support. Alternatively, if you are connecting within a private network such as a corporate Local Area Network (LAN), consult your system administrator.


Note: This chapter assumes both host and client computers are set up correctly. For more information, see *Getting VNC Enterprise Edition ready to use* on page 10.

Contents

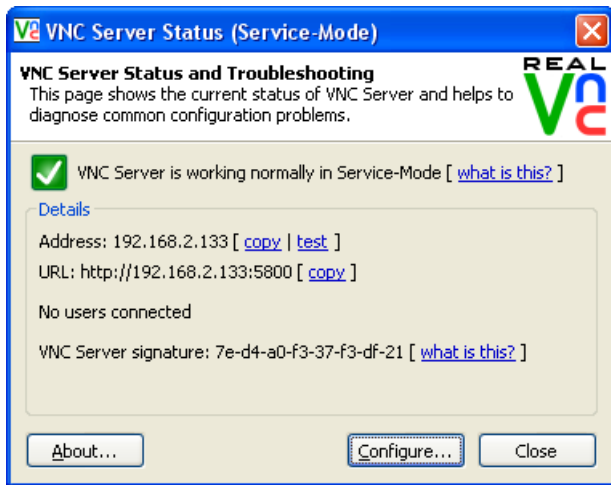
| | |
|---|----|
| Step 1: Ensure VNC Server is running on the host computer | 16 |
| Step 2: Start VNC Viewer on the client computer | 17 |
| Step 3: Identify VNC Server on the host computer | 17 |
| Step 4: Select an encryption option | 19 |
| Step 5: Connect and authenticate to VNC Server | 19 |
| Troubleshooting connection | 21 |

Step 1: Ensure VNC Server is running on the host computer

VNC Server may already be running on the host computer, but to make sure, and if you have access, follow the appropriate instructions for the host computer's platform below. If you do not have access, contact your system administrator or a host computer user.

- Under Windows, select **RealVNC > VNC Server** from the **Start** menu, or double-click the *VNC Viewer* desktop icon, if available. You may be required to confirm this operation.
- Under UNIX or Linux, either:
 - Type `x0vncserver` in a Terminal window, and press the ENTER key.
 - Select **Applications > Internet > VNC Server (User Mode)** from the menu system, if available.
- Under Mac OS X, navigate to the **Applications > RealVNC** folder, and double-click the **VNC Server** program. You may be required to confirm this operation. A *VNC Server* icon  appears in the Status Bar. Click this icon and select **Status** from the shortcut menu.

The **VNC Server Status** dialog opens:



(Windows XP)

If the green tick is visible, *VNC Server* should be running and configured correctly for new connections.

If an amber warning or red error is shown instead, click the [\[details\]](#) link that appears in the **Details** area, and start with *Troubleshooting connection* on page 21.

Step 2: Start VNC Viewer on the client computer

To start *VNC Viewer* on the client computer:

- Under Windows, select **RealVNC > VNC Viewer** from the **Start** menu.
- Under UNIX or Linux, either:
 - Type `vncviewer` in a Terminal window, and press the ENTER key.
 - Select **Applications > Internet > VNC Viewer** from the menu system, if available.
- Under Mac OS X, navigate to the **Applications > RealVNC** folder, and double-click the **VNC Viewer** program.

The **VNC Viewer: New Connection** dialog opens:



(Windows XP)

Step 3: Identify VNC Server on the host computer

You must uniquely identify *VNC Server* running on the host computer you want to connect to.

If you are connecting within a private network such as a LAN, enter the network address of the host computer itself in the **VNC Server** dropdown. This address can take the following forms:

- A friendly *host name* for the host computer, for example `johndoe`. (Note this facility may not be available.)
- An IP address for the host computer in IPv4 format, for example `192.168.2.187`.
- An IP address for the host computer in IPv6 format within square brackets, for example `[2001:db8::1]`. (IPv6 may not be available.)

If you do not know the network address of the host computer, see *Connecting within a private network* on page 21.

If you are connecting over the Internet, for example to friends or family, and the host computer is protected by a router, then enter the network address of the *router* in the **VNC Server** dropdown instead. If you do not know the network address of a router, see *Connecting over the Internet* on page 22.

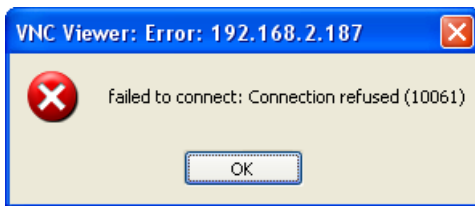
In the following example, the host computer is identified by an IPv4 network address:



(Windows XP)

Typically, a host computer needs no further identification. This is because, by default, *VNC Server* listens for network communications on a registered port, 5900. Carry on from *Step 4: Select an encryption option* on page 19.

There may be circumstances, however, when *VNC Server* is listening on a different port. This can occur if the host computer is running UNIX or Linux, or if more than one instance of *VNC Server* is running on the host computer. If, when you try to connect, you see an error message similar to the following:



then you probably need to qualify the network address with a port number. For more information, see *Qualifying a network address with a port number* on page 24.

Step 4: Select an encryption option

VNC Enterprise Edition is designed to be completely secure. By default, all communication between client and host computer is encrypted. For more information on security, see *Chapter 7, Security* on page 93.

By default, in the **VNC Viewer: New Connection** dialog, the **Encryption** dropdown is set to `Let VNC Server choose`:



(Windows XP)

It is recommended you retain this setting unless you have a good reason to turn encryption off.

Note: Encryption is ultimately controlled by *VNC Server*, whose default behavior is to encrypt. Selecting an alternative option such as `Prefer off` may not, in any case, have any effect. For more information, see *Relaxing the encryption rules* on page 105.

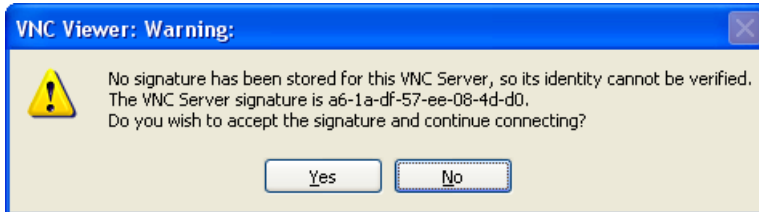
Step 5: Connect and authenticate to VNC Server

To connect to *VNC Server*, click the **Connect** button at the bottom of the **VNC Viewer: New Connection** dialog:



(Windows XP)

If this is the first time you have connected to *VNC Server* from this computer, a message similar to the following appears:

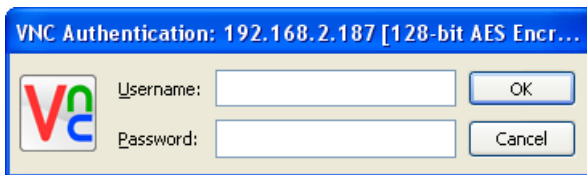


If you have access to the host computer, you can check that *VNC Viewer* is connecting to the correct host computer by comparing this signature with that displayed in the **VNC Server Status** dialog:

```
VNC Server signature: a6-1a-df-57-ee-08-4d-d0 [ what is this? ]
```

If you see any other message referring to the *VNC Server* signature, it is recommended you do *not* connect. For more information on this security feature, see *Uniquely identifying VNC Server* on page 114.

Click the **Yes** button to continue connecting to *VNC Server*. You may be required to enter a user name and password:



(Windows XP)

If so, then by default enter the credentials of a user with administrative privileges on the host computer. If you:

- Do not know this information and have access to the host computer, you may be able to find out, or alternatively register your own credentials.
- Know that the primary user account does not have a password set (likely for friends and family only), you must change the default authentication mechanism, or disable authentication altogether.

For more information, start with *Authenticating connections to VNC Server* on page 94. If you do not have access, contact a system administrator or a host computer user.

Click the **OK** button. If the connection is successful, *VNC Viewer* displays the host computer's desktop in a new window on the client computer. Carry on from *Connected: The VNC Viewer experience* on page 36. If the connection fails for any reason, start with *Troubleshooting connection* on page 21.

Note: Once connected, you can save a connection so you can quickly reconnect in future without having to remember the network address and authentication credentials. For more information, see *Appendix A, Saving Connections* on page 117.

Troubleshooting connection

The following sections provide additional information to help you connect.

If after reading this you still cannot connect, or if you want more information, consult the RealVNC web site, or contact Support. For details of these resources, see *About This Guide on page 7*.

If all else fails, and providing a host computer user is present, you can ask that person to connect to *you*. For more information, see *Establishing a reverse connection on page 104*.

Connecting within a private network

If both client and host computers are managed within a closed network environment such as a Local Area Network (LAN) or Virtual Private Network (VPN), you are connecting within a private network. This is common in corporate and other enterprise environments, and may also be the case if you are connecting two computers at home.

To connect within a private network, enter the network address of the host computer itself in the **VNC Viewer: New Connection** dialog, for example:



(Windows XP)

If you do not know the network address of the host computer:

- And you do not have access to it, you will need to consult your system administrator or a host computer user.
- And you *do* have access to it, follow the appropriate instructions for the host computer's platform below.

Windows

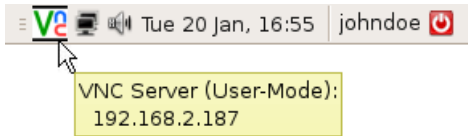
To discover the network address of a host computer, hover the mouse over the *VNC Server* icon in the Notification area. A tooltip containing a network address appears:



(Windows XP)

UNIX or Linux

To discover the network address of a host computer, hover the mouse over the *VNC Server* icon in the Notification Area. A tooltip containing a network address appears:

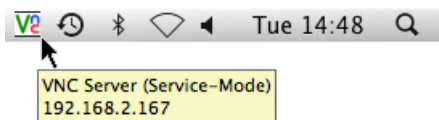


(Ubuntu 8.10 Linux)

Note: Under some versions of UNIX, a *VNC Server* icon is not available. You will have to use system tools to discover the network address.

Mac OS X

To discover the network address of a host computer, hover the mouse over the *VNC Server* icon in the Status Bar. A tooltip containing a network address appears:



(Mac OS X 10.5)

Connecting over the Internet

If you are connecting over the Internet, for example to friends and family, or in to the office on the move, it is likely that the host computer will be protected by a router or similar device acting as a communication gateway and public interface.

To connect over the Internet, you must enter the network address of the *router* in the **VNC Viewer: New Connection** dialog, for example:



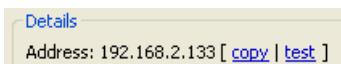
(Windows XP)

If you do not know the network address of a host computer's router:

- And you do not have access to the host computer, you will need to ask a host computer user to follow the instructions below, or to use a service such as www.whatismyip.com.
- And you *do* have access to the host computer, follow the instructions below.

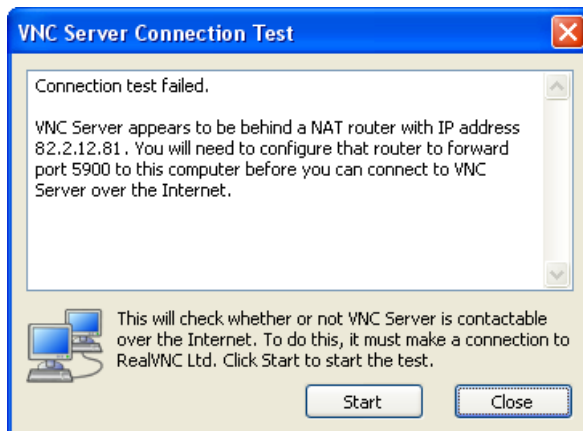
To discover the network address of a router:

1. Open the **VNC Server Status** dialog.
2. In the **Details** area, click the [\[test\]](#) link:



The **VNC Server Connection Test** dialog appears.

3. Click the **Start** button. RealVNC attempts to contact the host computer over the Internet. Providing the host computer is connected to the Internet, the network address of an intermediary device is revealed:



(Windows XP)

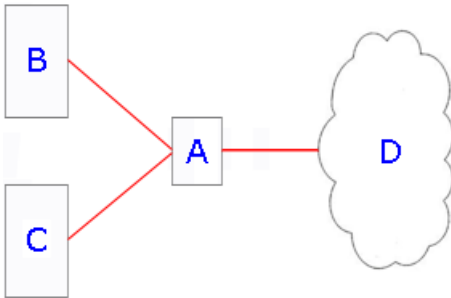
Configuring a router to forward network communications

In a typical home or small office environment, a router assigns a private network address to an internal computer. You should also be aware that *VNC Server* listens for network communications on a particular port. The router must be configured to forward communications from *VNC Viewer* to the correct port at the correct private network address. This procedure is known as port forwarding.

Note: Port forwarding instructions are specific to routers. If you do not have access to the host computer, ask a host computer user to consult the manufacturer's documentation, or visit www.portforward.com.

Note that a router may act as a public interface to more than one computer in a home or small office environment. If you want to connect to multiple host computers, then *VNC Server* must be running on each and listening on a different port. The router must be configured to distinguish between host computers using port numbers.

Consider the following example:



A. Router with a network address assigned by an ISP, for example 82.2.12.81. **B.** Host computer with a network address assigned by the router, for example 192.168.0.1. VNC Server is listening on the default port, 5900. **C.** Host computer with a network address assigned by the router, for example 192.168.0.2. VNC Server has been configured to listen on port 5901. **D.** The Internet.

In this scenario, the router must be configured to forward port 5900 to host computer B at 192.168.0.1 and port 5901 to host computer C at 192.168.0.2.

When you connect to either host computer from *VNC Viewer*, you must enter the network address of the router: 82.2.12.81. In addition, to connect to host computer C, you must qualify the router's network address with the port number: 82.2.12.81:1. To find out why this is, see *Qualifying a network address with a port number* on page 24.

Qualifying a network address with a port number

VNC Server listens for network communications on a particular *port*. By default, and providing it is available when *VNC Server* starts, this is port 5900 for connection requests. This port is registered for use by *VNC Server* with the Internet Assigned Numbers Authority (IANA).

Note: For more information on ports, see *Configuring network communications* on page 86.

If *VNC Server* is listening on any other port, you must qualify the network address of the host computer (or router) with the port number when you connect from *VNC Viewer*, for example:



(Windows XP)

If you know that *VNC Server* is listening on a port between 5901 and 5999, append a colon (:) and an identifying number (1 through 99) to the network address, for example:

```
johndoe:1
192.168.2.187:1
[2001:db8::1]:1
```

If you know that *VNC Server* is listening on any other port, append a double colon (: :) and the full port number to the network address, for example:

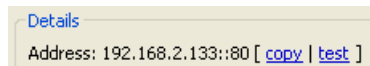
```
johndoe::6001
192.168.2.187::6001
[2001:db8::1]::6001
```

If you do not know on which port *VNC Server* is listening:

- And you do not have access to the host computer, you will need to consult your system administrator or a host computer user.
- And you *do* have access to the host computer, follow the appropriate instructions for its platform below.

Windows

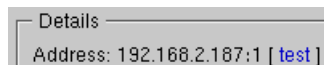
To see whether *VNC Server* is listening on a port other than 5900, double-click the *VNC Server* icon in the Notification area to open the **VNC Server Status** dialog. If applicable, this information is appended to the network address in the **Details** area:



In this example, *VNC Server* is running on host computer 192.168.2.133 and listening on port 80.

Unix or Linux

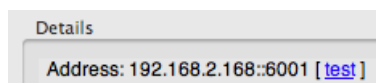
To see whether *VNC Server* is listening on a port other than 5900, click the *VNC Server* icon in the Notification Area to open the **VNC Server Status** dialog. If applicable, this information is appended to the network address in the **Details** area:



In this example, *VNC Server* is running on host computer 192.168.2.187 and listening on port 5901.

Mac OS X

To see whether *VNC Server* is listening on a port other than 5900, click the *VNC Server* icon and, from the shortcut menu, select **Status** to open the **VNC Server Status** dialog. If applicable, this information is appended to the network address in the **Details** area:

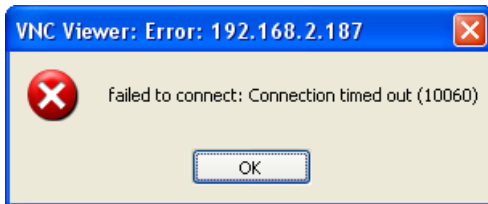


In this example, *VNC Server* is running on host computer 192.168.2.168 and listening on port 6001.

Allowing network communications through a firewall

If the host computer is protected by a firewall, then the firewall must be configured to allow incoming network communications to the port on which *VNC Server* is listening. To find out which port this is, see *Qualifying a network address with a port number* on page 24.

The firewall might be automatically configured by the operating system of the host computer. If not, you will probably see the following error message when you connect from *VNC Viewer*:



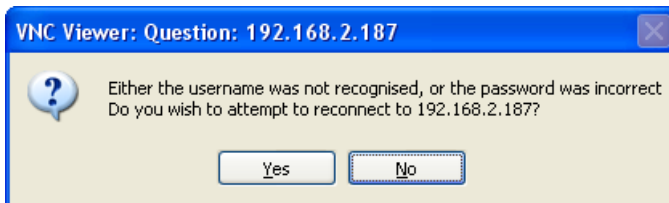
The instructions for adding exceptions for ports are specific to firewalls. If you do not have access to the host computer, ask a host computer user to consult the manufacturer's documentation.

Miscellaneous connection messages

This section explains various error or warning messages you might see.

Failing to authenticate correctly

If you see the following warning message:

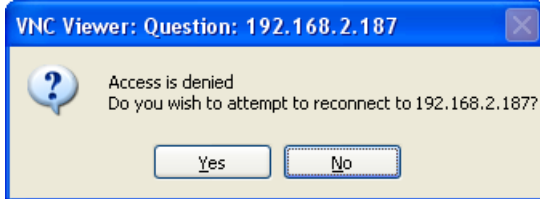


then you have not authenticated yourself correctly to *VNC Server*. Note that user names and passwords are case-sensitive. Click the **Yes** button to try again up to four more times.

If you do not know the correct user name or password, and you do not have access to the host computer, you will need to consult your system administrator or a host computer user. If you *do* have access to the host computer, and sufficient privileges to configure *VNC Server*, you may be able to relax the authentication rules. For more information, see *Relaxing the authentication rules* on page 99.

Failing to authenticate as 'you'

If you see the following warning message:



then *VNC Server* has been configured to authenticate a *VNC Viewer* user with the credentials used for *logging on* to the operating system of the host computer. *Your* user name and password for logging on to the host computer, however, have not been added to the authentication list.

If this is the case and you do not have access to the host computer, you will need to consult your system administrator or a host computer user. If you *do* have access to the host computer, and sufficient privileges to configure *VNC Server*, you may be able to register your credentials. For more information, see *Managing users and groups in the authentication list* on page 98.

Connecting from an unauthorized computer

If you see the following error message:



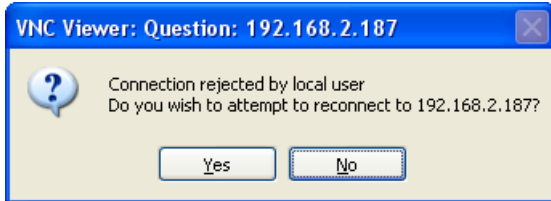
then it could be that *VNC Server* has been configured to prevent connections from the client computer you are using.

If this is the case and you do not have access to the host computer, you will need to consult your system administrator or a host computer user. If you *do* have access to the host computer, and sufficient privileges to configure *VNC Server*, you may be able to unblock your client computer. For more information, see *Preventing connections from particular client computers* on page 106.

Alternatively, you may be able to connect from a different client computer.

Being rejected by a host computer user

If you see the following warning message:



then *VNC Server* has been configured to display connection prompts to a host computer user, and your request has either been explicitly rejected, or has timed out (this could either be because the prompt was deliberately ignored, or because no host computer user is actually present).

If this is the case and you do not have access to the host computer, you will need to consult your system administrator or a host computer user. If you *do* have access to the host computer, and sufficient privileges to configure *VNC Server*, you may be able to bypass host computer connection prompts. For more information, see *Preventing particular users connecting* on page 108.

3

Using VNC Viewer

This chapter explains how to connect to *VNC Server* and control a host computer using *VNC Viewer*, and how *VNC Viewer* features can enhance your productivity while a connection is in progress.

Note: This chapter assumes you are using fully-featured—and not standalone—*VNC Viewer*. For more information, see *VNC Enterprise Edition 4.5 connectivity* on page 12.

Contents

| | |
|--|----|
| Starting VNC Viewer | 30 |
| Configuring VNC Viewer before you connect | 31 |
| Connecting to a host computer | 35 |
| Connected: The VNC Viewer experience | 36 |
| Using the VNC Viewer toolbar | 38 |
| Using the VNC Viewer shortcut menu | 39 |
| Using the VNC Viewer Properties dialog | 41 |
| Managing the current connection | 42 |
| Changing the appearance and behavior of VNC Viewer | 43 |
| Restricting access to functionality | 45 |

Starting VNC Viewer

To start *VNC Viewer* on the client computer:

- Under Windows, select **RealVNC > VNC Viewer** from the **Start** menu, or double-click the *VNC Viewer* desktop icon, if available.
- Under UNIX or Linux, either:
 - Type `vncviewer` in a Terminal window, and press the ENTER key.
 - Select **Applications > Internet > VNC Viewer** from the menu system, if available.
- Under Mac OS X, navigate to the **Applications > RealVNC** folder, and double-click the **VNC Viewer** program.

The **VNC Viewer: New Connection** dialog opens:



(Windows XP)

VNC Viewer is ready to connect to *VNC Server* out-of-the-box. However, if you want to configure it, note that some properties must be configured *before* you connect. For more information, see *Configuring VNC Viewer before you connect* on page 31.


To carry on connecting to a host computer, see *Connecting to a host computer* on page 35.

Starting Listening VNC Viewer

You can start *VNC Viewer* in such a way that it does not connect to *VNC Server* but rather waits for *VNC Server* to connect to it. This is called a *reverse connection*. For more information about this feature, and why you might want to use it in conjunction with a host computer user, see *Establishing a reverse connection* on page 104.

To start *Listening VNC Viewer*:

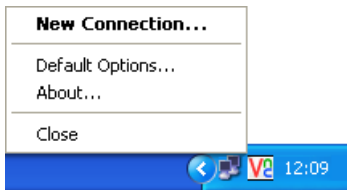
- Under Windows, select **RealVNC > Advanced > Start Listening VNC Viewer** from the **Start** menu.
- Under UNIX or Linux, type `vncviewer -listen` in a Terminal window, and press the ENTER key. Note that the Terminal window must stay open while a reverse connection is in progress.
- Under Mac OS X, navigate to the **Applications > RealVNC** folder, and double-click the **VNC Viewer** program. The **VNC Viewer** application menu opens. Select **VNC Viewer > Launch Listening VNC Viewer**.

Under Windows or Mac OS X, a *VNC Viewer* icon  is displayed in the Notification area and Dock respectively. Hover the mouse cursor over the icon to confirm that *Listening VNC Viewer* is running:



(Windows XP)

Under Windows, *Listening VNC Viewer* has a shortcut menu:



(Windows XP)

You do not need to configure *Listening VNC Viewer*, but if you want to do so before a connection is established, select **Default Options** to open the **VNC Viewer Defaults** dialog. This dialog contains the same properties as the **VNC Viewer Properties** dialog. For more information, start with *Configuring VNC Viewer before you connect* on page 31.

Note you can select **New Connection** to open the **VNC Viewer: New Connection** dialog and use *VNC Viewer* to establish a connection to *VNC Server* in the normal way. Carry on from *Connecting to a host computer* on page 35.

If a reverse connection is successfully established, *Listening VNC Viewer* displays the host computer's desktop in a new window on the client computer in exactly the same way as *VNC Viewer*. Carry on from *Connected: The VNC Viewer experience* on page 36.

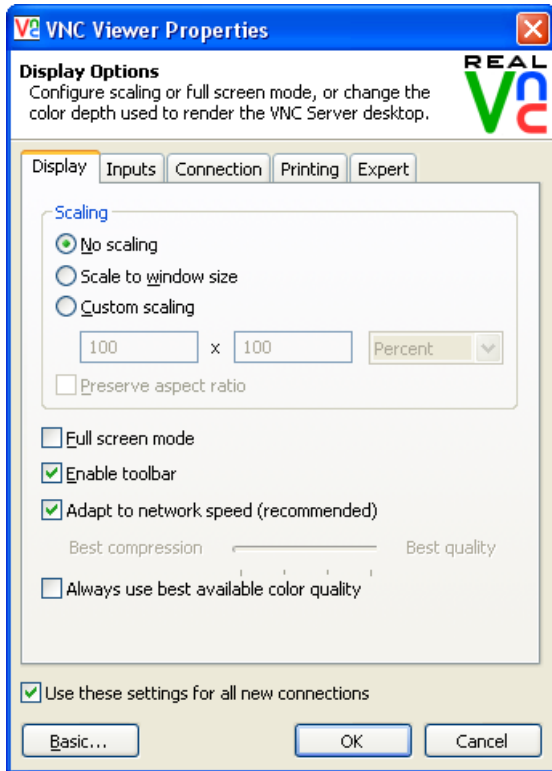
If a reverse connection is not successful, start with *Establishing a reverse connection* on page 104.

Configuring VNC Viewer before you connect

VNC Viewer is ready to connect to *VNC Server* and control a host computer out-of-the-box. You do not need to configure it. However, you can change almost any aspect to suit your requirements and environment if you wish.

Some properties must be configured before you connect. Most, however, can be configured once you are connected, and changes applied to the current connection. By default, any changes you make are applied to all future connections as well.

To configure *VNC Viewer* before you connect, click the **Options** button on the **VNC Viewer: New Connection** dialog. For more information on this dialog, see *Starting VNC Viewer* on page 30. The **VNC Viewer Properties** dialog opens:



(Windows XP. In this example, the dialog is in Advanced mode.)

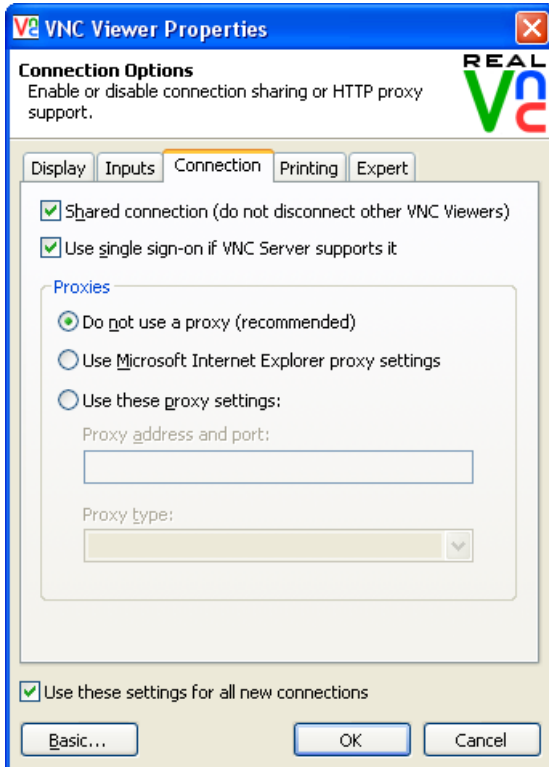
The first time you open this dialog, it opens in Basic mode, and only one tab is available. Click the **Advanced** button in the bottom left corner to switch to Advanced mode and see all the tabs in the example above.

The **Connection** and **Printing** tabs are only available before you connect. The other tabs are available all the time (in Advanced mode). For more information, see *Using the VNC Viewer Properties dialog* on page 41.

By default, any changes you make are remembered for all future connections to any host computer. To apply them just to the next connection, turn off **Use these settings for all new connections**.

Configuring connections

You can configure connections using the properties on the **Connection** tab:



(Windows XP)

Disconnecting other users

By default, if other users are connected when you connect, you share control of the host computer's desktop. Operations may occur unexpectedly!

To disconnect other users when you connect, turn off **Shared connection (do not disconnect other VNC Viewers)**. Note that you may be disconnected in turn.

Disabling single sign-on (Windows and Mac OS X only)

By default, if *VNC Server* specifies `Single sign-on` as its authentication mechanism, then you may be able to connect without supplying a user name and password. This is because you have already successfully authenticated when logging on to the client computer. For more information, see *Relaxing the authentication rules* on page 99.

You can disable this feature if you want to connect to *VNC Server* using a different user name and password. This might give you access to more VNC functionality. To do this, turn off **Use single sign-on if VNC Server supports it**. You will need to know the user name and password of a valid host computer user.

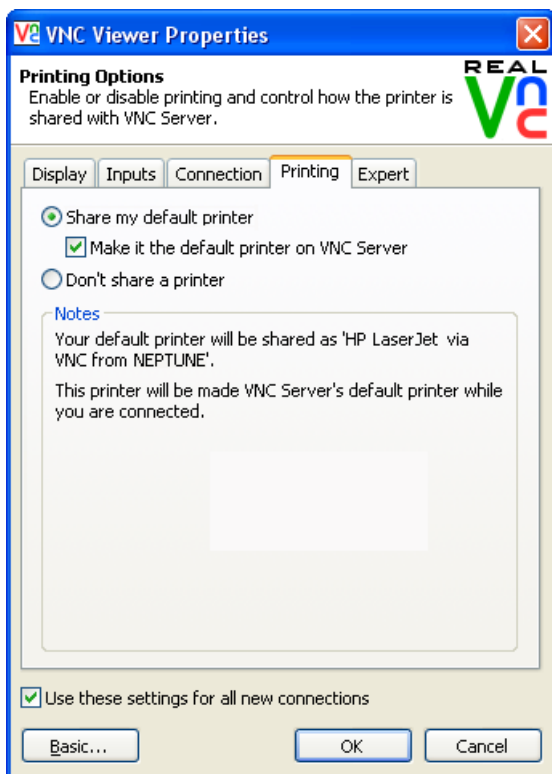
Using a proxy server

If you are connecting over the Internet and your client computer uses a proxy server, you must tell VNC Viewer about the proxy server. You can either:

- Use the proxy server already set up for your system. To do this, choose **Use Microsoft Internet Explorer proxy settings**. (This option has a different name under UNIX or Linux and Mac OS X.)
- Set up a new proxy server. To do this, choose **Use these proxy settings**, and enter the details.

Configuring printing

You can configure printing using the properties on the **Printing** tab:



(Windows XP)

By default, when you connect, the client computer's default printer (if it has one) is shared with the host computer and made *its* default while the connection is in progress. This means you can print host computer files directly to a printer attached to your client computer. For more information about this feature, see *Printing host computer files to a local printer* on page 60.

You can print but choose not to change the host computer's default printer. This means you will have to explicitly select your printer when you print. To do this, turn off **Make it the default printer on VNC Server**.

To disable printing, choose **Don't share a printer**.

Connecting to a host computer

This section summarizes how to connect from a client computer running *VNC Viewer* to a host computer running *VNC Server*. For a step-by-step guide, see *Chapter 2, Getting Started: Connecting A Client To A Host Computer* on page 15.

1. Start *VNC Viewer* on the client computer. The **VNC Viewer: New Connection** dialog opens.
2. In the **VNC Server** dropdown, enter a network address for the host computer (this may be a router), qualified, if applicable, by the port number on which *VNC Server* is listening, for example
192.168.2.187:1.
3. From the **Encryption** dropdown, select an encryption option, or retain the default: Let *VNC Server* choose.
4. Click the **Connect** button.

You may be asked to confirm a signature that uniquely identifies *VNC Server*. You may also be asked to authenticate yourself to *VNC Server*.

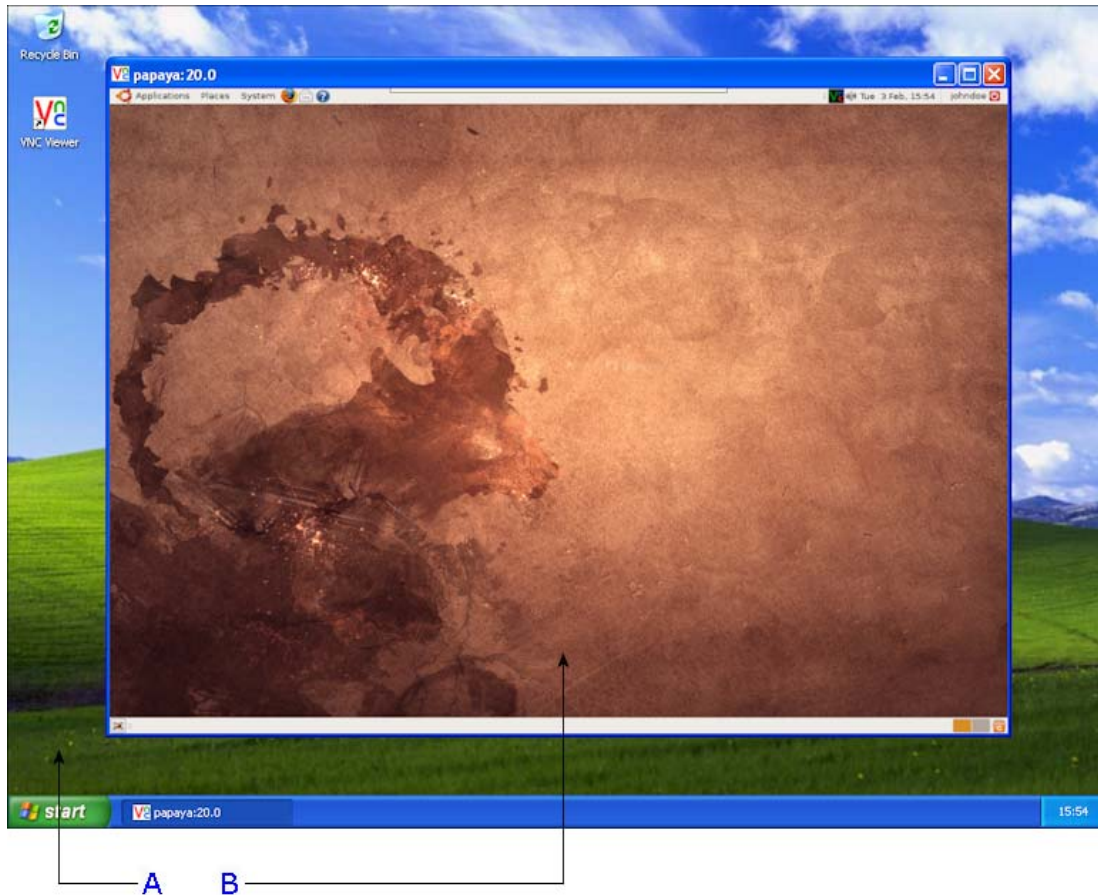
If the connection is successful, *VNC Viewer* displays the host computer's desktop in a new window on the client computer. Carry on from *Connected: The VNC Viewer experience* on page 36. If the connection fails for any reason, start with *Troubleshooting connection* on page 21.

Note: Once connected, you can save a connection so you can quickly reconnect in future without having to remember the network address and authentication credentials. For more information, see *Appendix A, Saving Connections* on page 117.

Connected: The VNC Viewer experience

The rest of the sections in this chapter assume you are successfully connected to a host computer. If not, see *Connecting to a host computer* on page 35.

When a connection is established, *VNC Viewer* displays the host computer's desktop in a new window on the client computer:



A. Desktop of a client computer running Windows XP. **B.** VNC Viewer displaying the desktop of a host computer running Ubuntu 8.10 Linux.

Note: If the host computer is running UNIX or Linux, *VNC Viewer* may display a *virtual* desktop instead, in which case what you see is *not* the desktop of a host computer user. For more information on this feature, see *Running multiple instances of VNC Server* on page 76.

Controlling the host computer using your keyboard and mouse

The client computer's keyboard and mouse are now shared with the host computer. This means that:

- Moving the mouse and clicking within the *VNC Viewer* window affects the host computer and not the client.
- Moving the mouse and clicking outside the *VNC Viewer* window, or on the *VNC Viewer* title bar or window buttons (**Minimize**, **Maximize**, and **Close**), affects the client computer and not the host.

The same applies to the client computer's keyboard with the exception of the function key that opens the shortcut menu (F8 by default), and the CTRL-ALT-DELETE key combination. These are interpreted by the client computer. Alternative ways of sending these are available; see *Using the VNC Viewer shortcut menu* on page 39 for more information. Under *Windows*, you can configure *VNC Viewer* to specify that *other* key presses are also interpreted by the client computer; see *Changing the appearance and behavior of VNC Viewer* on page 43 for more information.

Note: If your keyboard and mouse have no effect on the host computer, they may have been disabled. For more information, see *Restricting access to functionality* on page 45.

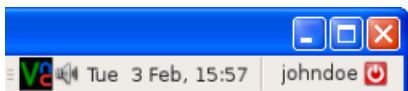
Note that it is possible for the client and host computers to have different types of keyboard. Not all the keys available to a host computer user may be available to you, and some keys with the same name may have different behavior. This is especially likely if you are connecting to a Mac OS X host from a Windows or Linux client with a PC keyboard, or *vice versa*. For more information on key mapping, consult the RealVNC web site.

If the client and host computers have different numbers of mouse buttons, you can configure *VNC Viewer* to emulate those you do not have. For more information, see *Changing the appearance and behavior of VNC Viewer* on page 43.

Note: Other *VNC Viewer* users may be connected to the host computer and controlling it at the same time as you. In addition, a host computer user may be present. Operations may occur unexpectedly!

Interacting with VNC Server

When you connect, a *VNC Server* icon  is displayed on the host computer's desktop, shaded black:



(*Windows XP client computer, Ubuntu 8.10 Linux host*)

Note: Under UNIX or Linux, in some circumstances, the *VNC Server* icon is not shaded black. Under some versions of UNIX, it is not available at all.

The *VNC Server* icon confirms that *VNC Server* is running on the host computer, provides information to help *VNC Viewer* users connect, confirms that at least one *VNC Viewer* user is connected (the icon turns black), and has a shortcut menu to perform useful operations. All this information and functionality is available to you as a connected user. For more information, see *Working with VNC Server* on page 79.

Note that the *VNC Server* icon also provides access to *VNC Server* properties. However, you cannot configure *VNC Server* unless logged on as a host computer user with administrative privileges. For more information, see *Authenticating connections to VNC Server* on page 94.

Using the VNC Viewer toolbar

VNC Viewer has a toolbar to facilitate common operations.

Note: If you cannot access the VNC Viewer toolbar, it may have been disabled. For more information, see *Changing the appearance and behavior of VNC Viewer* on page 43.

Under Windows and UNIX or Linux, the VNC Viewer toolbar is located at the top center of the VNC Viewer window. To use it, hover the mouse over the hot area:















(Windows XP)

Note: Under Mac OS X, the VNC Viewer toolbar is located across the top of the window and is always visible. Buttons may appear slightly different to those in the example below, but the behavior is the same.



The following table explains the effect of clicking each toolbar button.

| | Button name | Explanation |
|---|--------------------------|---|
|  | New Connection | Opens the VNC Viewer: New Connection dialog. You can start a new connection to the same host computer, or to a different one. Carry on from <i>Connecting to a host computer</i> on page 35. |
|  | Save Connection | You can save the current connection so you can quickly reconnect in future without having to remember the network address and your authentication credentials. For more information, see <i>Appendix A, Saving Connections</i> on page 117. |
|  | Close Connection | Prompts you to close the current connection (and the VNC Viewer window). |
|  | Options | Opens the VNC Viewer Properties dialog. You can configure most aspects of VNC Viewer while the current connection is in progress. For more information, see <i>Using the VNC Viewer Properties dialog</i> on page 41. Note that some properties must be configured before you connect. For more information, see <i>Configuring VNC Viewer before you connect</i> on page 31. |
|  | Full Screen Mode | Toggles full screen mode on and off. |
|  | Send Ctrl-Alt-Del | Sends the CTRL-ALT-DELETE command to the host computer. (Pressing this key combination would be interpreted by the client computer.) You could alternatively press SHIFT-CTRL-ALT-DELETE. |
|  | Send Files To VNC Server | Opens a dialog where you can browse to the location of client computer files to send to the host computer. For more information, see <i>Transferring files between client and host computers</i> on page 62. |

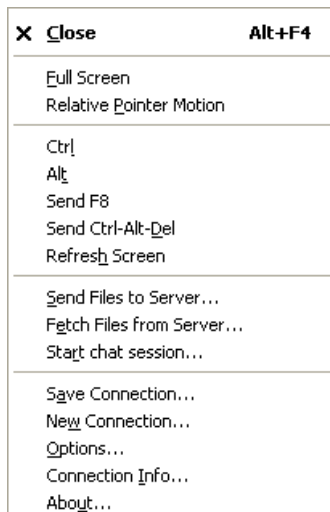
| | Button name | Explanation |
|---|-----------------------------|--|
|  | Fetch Files From VNC Server | This option is only available if the host computer has made files available for the client computer to fetch. A dialog opens where you can browse to a location to put shared host computer files. For more information, see <i>Transferring files between client and host computers</i> on page 62. |
|  | Start Chat Session | Opens dialogs enabling you to chat with other VNC Viewer users connected to the same host computer, or with a host computer user. For more information, see <i>Communicating securely using VNC Chat</i> on page 67. |
|  | Connection Information | Opens a dialog displaying technical information about the current connection, such as the encryption method and compression format. |
|  | encryption | The connection is encrypted/not encrypted (only one of these buttons is shown). |
|  | connection speed/activity | Hovering over this toolbar button reveals the current connection speed. For more information on performance, see <i>Changing the appearance and behavior of VNC Viewer</i> on page 43. |

Using the VNC Viewer shortcut menu

VNC Viewer has a shortcut menu that facilitates many of the same common operations as the VNC Viewer toolbar. For more information on this, see *Using the VNC Viewer toolbar* on page 38.

Note: If you cannot access the VNC Viewer shortcut menu, it may have been disabled. For more information, see *Changing the appearance and behavior of VNC Viewer* on page 43.

By default, to open the shortcut menu, press the F8 key (you may need to hold down the FN key under Mac OS X):



(Windows XP. Some standard Windows menu options have been omitted from this example.)

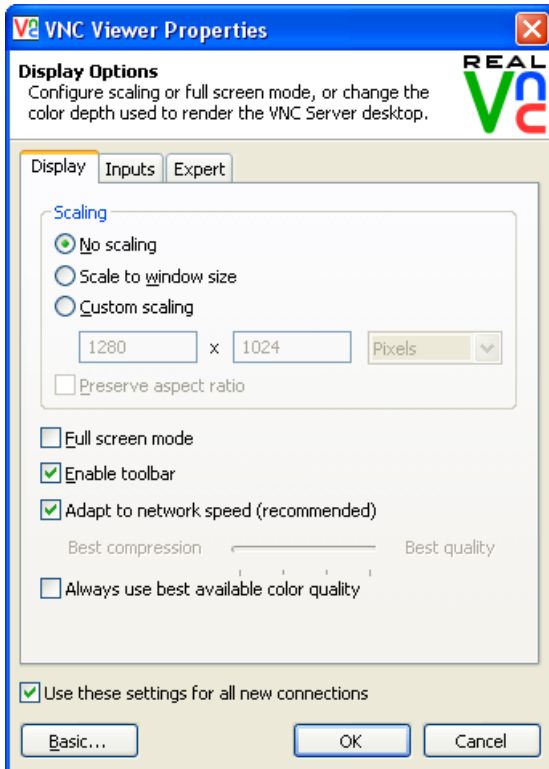
Note: Under Mac OS X, more **Send <key>** options are available to send Mac-specific commands to a host computer also running Mac OS X.

The following table explains the effect of selecting menu options that do not have equivalent toolbar buttons.

| Shortcut menu option | Explanation |
|-------------------------|--|
| Relative Pointer Motion | Turn this option on if the host computer's mouse cursor appears to be behaving abnormally, for example by accelerating too fast. |
| Ctrl | Turn this option on to simulate holding down the CTRL key. |
| Alt | Turn this option on to simulate holding down the ALT key. |
| Send F8 | Sends an F8 command to the host computer. (By default, F8 opens the shortcut menu; see <i>Changing the VNC Viewer shortcut menu key</i> on page 45 for information on choosing a different key.) You could alternatively press F8 twice in quick succession. |
| Refresh Screen | Refreshes the display of the host computer's desktop. |
| About | Displays <i>VNC Viewer</i> version information. You may need this if you contact Support. |


Using the VNC Viewer Properties dialog

The **VNC Viewer Properties** dialog allows you to configure *VNC Viewer* while a connection is in progress:



(Windows XP. In this example, the dialog is in Advanced mode.)

Note: Some *VNC Viewer* properties must be configured *before* you connect. For more information, see *Configuring VNC Viewer before you connect* on page 31.

To open the **VNC Viewer Properties** dialog, click the **Options**  toolbar button, or select **Options** from the shortcut menu. (If the *VNC Viewer* toolbar or shortcut menu are not accessible, see *Changing the appearance and behavior of VNC Viewer* on page 43.)

The first time you open this dialog, it opens in Basic mode, and only one tab is available, containing the most common properties. Click the **Advanced** button in the bottom left corner to switch to Advanced mode and see all the tabs in the example above. Note that the **Expert** tab is recommended for expert users only.

By default, any changes you make apply both to the current connection *and to all future connections to any host computer*. To apply changes just to the current connection, turn off **Use these settings for all new connections** first.

The rest of the sections in this chapter explain the properties in this dialog.

Managing the current connection

You can manage aspects of the current connection while it is in progress.


Note: Most of the operations described in this section are facilitated by the *VNC Viewer* toolbar. For more information on this, see *Using the VNC Viewer toolbar* on page 38.

Saving the current connection

You can save the current connection so you can quickly reconnect in future without having to remember the network address and your authentication credentials. In addition, your preferred *VNC Viewer* environment for controlling the host computer is automatically recreated.


To save the current connection, click the **Save Connection**  toolbar button. Carry on from *Appendix A, Saving Connections* on page 117.

Starting a new connection

You can start a new connection to the same host computer, or to a different one. To do this, click the **New Connection**  toolbar button. The **VNC Viewer: New Connection** dialog opens. Carry on from *Connecting to a host computer* on page 35.

By default, any properties you have configured are inherited by the new connection. To prevent this, open the **VNC Viewer Properties** dialog and turn off **Use these settings for all new connections** first. For more information on this dialog, see *Using the VNC Viewer Properties dialog* on page 41.

Closing the current connection

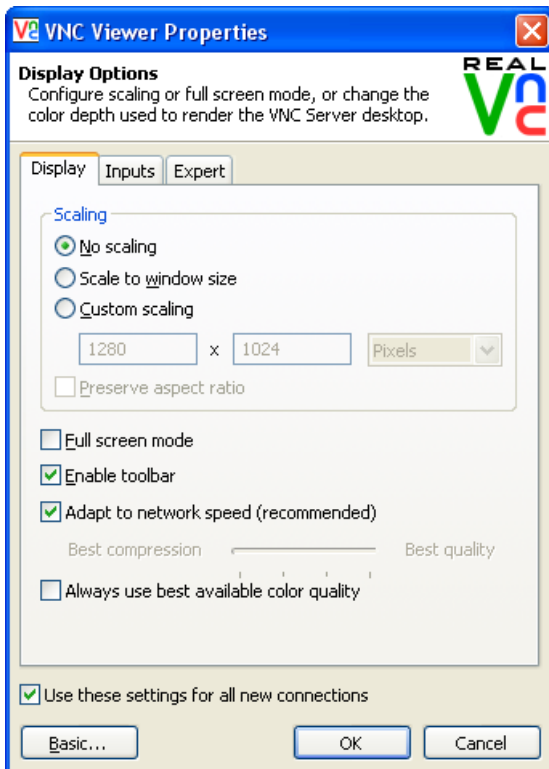
You can quickly close the current connection. To do this, click the **Close Connection**  toolbar button. You are prompted to confirm the operation before the *VNC Viewer* window closes.

Changing the appearance and behavior of VNC Viewer

By default, when a connection is established:

- VNC Viewer does not scale the host computer's desktop. Instead, scroll bars are added to the window if the desktop is too large.
- VNC Viewer displays the host computer's desktop at a color quality appropriate to the network connection speed.
- Your mouse and keyboard are set to interact with the client and host computers in particular ways.
- The VNC Viewer window is set to a particular size.
- The VNC Viewer toolbar is accessible.
- The VNC Viewer shortcut menu is accessible (by pressing F8).

You can change these defaults by configuring properties on the **Display** tab of the **VNC Viewer Properties** dialog. For more information on this dialog, see *Using the VNC Viewer Properties dialog* on page 41.



(Windows XP)

Scaling the host computer's desktop

You can scale the host computer's desktop, which might make it easier to navigate and to use.

To scale the desktop to the size of the *VNC Viewer* window, choose **Scale to window size**.

To scale it to a custom size, choose **Custom scaling**, and specify a width and height for the *VNC Viewer* window. Turn on **Preserve aspect ratio** to automatically calculate a height for a given width, and *vice versa*. Note you cannot resize a custom-sized *VNC Viewer* window using your mouse.

Trading performance for picture quality

You may be able to enhance the performance of *VNC Viewer* by reducing the number of colors used to display the host computer's desktop. To do this, turn off **Adapt to network speed (recommended)**, and move the slider towards **Best compression**.

If you want to enhance performance but retain full color, turn on **Always use best available color quality**. Performance is enhanced by other means, for example by reducing the amount of information sent about the mouse cursor's position. Note this may make mouse cursor movements appear jerky on the host computer.

Note: You can explicitly reduce the amount of mouse cursor position information sent by turning on **Rate-limit mouse move events**. This property is on the **Inputs** tab. This may also be useful if you are connecting over a mobile or dial-up network.

Configuring your mouse (Windows and Mac OS X only)

You can emulate buttons missing because your mouse has fewer buttons than the host computer's mouse.

To do this, turn on **Enable 3-button mouse emulation**. To emulate the missing middle button, click the left and right mouse buttons simultaneously. Under Mac OS X, you can also, or alternatively, turn on **Enable 2-button mouse emulation**. To emulate the missing right button, hold down the CTRL key and press the button. Note these properties are on the **Inputs** tab.

Configuring your keyboard (Windows only)

By default, and with the exception of CTRL-ALT-DELETE and the function key used to open the shortcut menu, key presses affect the host computer and not the client. To reverse this behavior for the application-level keys listed below, turn off **Pass special keys directly to VNC Server**. Note this property is on the **Inputs** tab.

Affected keys/combinations: WINDOWS (also known as START), PRINT SCREEN, ALT-TAB, ALT-ESCAPE, CTRL-ESCAPE.

Changing the size of the VNC Viewer window

You can use the mouse to resize the *VNC Viewer* window in the expected way for the platform of the client computer. The window's Application buttons (**Minimize**, **Maximize**, and **Close**) also work in the expected way.

To toggle full screen mode on and off, click the **Full Screen Mode**  *VNC Viewer* toolbar button.

Disabling the VNC Viewer toolbar (Windows and UNIX or Linux only)

You can disable the *VNC Viewer* toolbar. For more information on this, see *Using the VNC Viewer toolbar* on page 38. To do this, turn off **Enable toolbar**.

Note that if you disable the *VNC Viewer* shortcut menu as well you will not be able to access the *VNC Viewer* toolbar again while the current connection is in progress.

Disabling the VNC Viewer shortcut menu (Windows and UNIX or Linux only)

You can disable the *VNC Viewer* shortcut menu. For more information on this, see *Using the VNC Viewer shortcut menu* on page 39. To do this, select `none` from the **Menu key** dropdown. Note this property is on the **Inputs** tab.

Note that if you disable the *VNC Viewer* toolbar as well you will not be able to access the *VNC Viewer* shortcut menu again while the current connection is in progress.

Changing the VNC Viewer shortcut menu key

You can change the function key used to open the shortcut menu. To do this, select a function key from the **Menu key** dropdown. Note this property is on the **Inputs** tab. The shortcut menu updates to reflect the fact that you can no longer press the chosen key to send a command to the host computer.

Restricting access to functionality

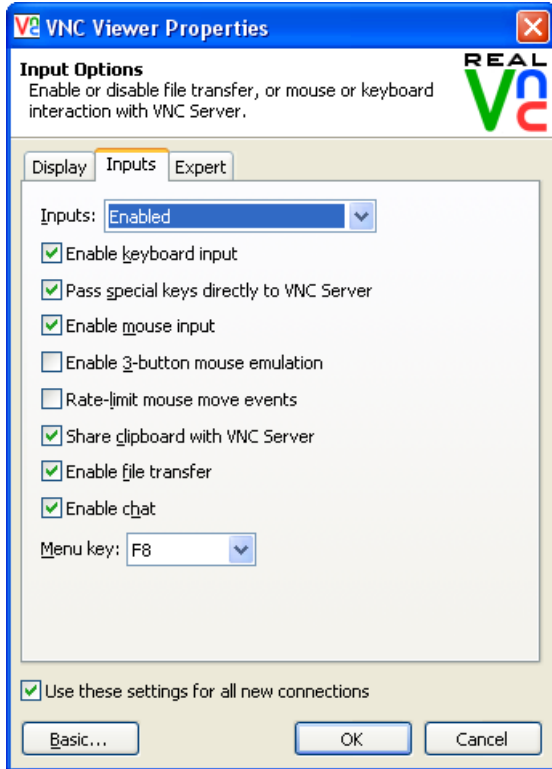
By default, while a connection is in progress, you should be able to:

- Control the host computer using your keyboard and mouse.
- Print host computer files directly to a local printer.
- Exchange files with the host computer.
- Copy and paste text between applications running on the client and host computers.
- Chat with other *VNC Viewer* users connected to the same host computer, or with a host computer user.

VNC Server may have been configured to prevent some or all of these operations. For more information, see *Restricting functionality for connected users* on page 90. In addition, *VNC Viewer* might have been configured to disable printing before the connection started.

You can restrict access to *VNC Enterprise Edition* functionality while the connection is in progress by configuring properties on the **Inputs** tab of the **VNC Viewer Properties** dialog. For more information on this dialog, see *Using the VNC Viewer Properties dialog* on page 41. You might want to do this if you are watching a demonstration on the host computer, for example, and want to prevent inadvertent interruption.

Note: You can enable functionality again at any time. To prevent this for the current connection only, disable the *VNC Viewer* toolbar and shortcut menu. For more information, see *Changing the appearance and behavior of VNC Viewer* on page 43.



(Windows XP)

Making VNC Viewer ‘view only’

You can quickly prevent all interchange with the host computer, making *VNC Viewer* ‘view only’. To do this, select *Disabled (view-only mode)* from the **Inputs** dropdown.

Disabling your keyboard

You can disable the client computer’s keyboard. To do this, turn off **Enable keyboard input**.

Disabling your mouse

You can disable the client computer’s mouse. To do this, turn off **Enable mouse input**.

Disabling file transfer

You can disable file transfer between client and host computers. To do this, turn off **Enable file transfer**.

For more information about this feature, see *Transferring files between client and host computers* on page 62.

Disabling copy and paste

You can disable copy and paste between applications running on the client and host computers. To do this, turn off **Share clipboard with VNC Server**.

For more information about this feature, see *Copying and pasting text between client and host computers* on page 66.

Disabling VNC Chat

You can disable *VNC Chat*. To do this, turn off **Enable chat**. For more information about this feature, see *Communicating securely using VNC Chat* on page 67.

4

Connecting From A Web Browser

This chapter explains how to connect to *VNC Server* and control a host computer using *VNC Viewer for Java*. All you need to do this is a Java-enabled web browser; you do not need to install or run any programs. This may be useful if you are at an Internet café, for example.

VNC Viewer for Java establishes an encrypted, authenticated connection to a host computer in the same way as *VNC Viewer*. You can use your mouse and keyboard to control the host computer exactly as you would using *VNC Viewer*. Note, however, that not all of *VNC Viewer*'s functionality is available.

Note: For more information on differences with *VNC Viewer*, start with *VNC Enterprise Edition 4.5 connectivity* on page 12.

Contents

| | |
|---|----|
| Connecting to a host computer | 50 |
| Connected: The VNC Viewer for Java experience | 54 |
| Working with VNC Viewer for Java | 55 |

Connecting to a host computer

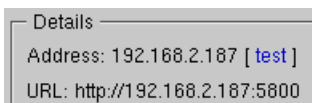
Connecting to a host computer is a two-stage process using *VNC Viewer for Java*.

Downloading VNC Viewer for Java

The first stage is to download *VNC Viewer for Java*. To do this:

1. Start a Java-enabled web browser on the client computer. For more information on what this means, see www.java.com.
2. In the URL bar, enter `http://` and a network address for the host computer, qualified by the port number on which *VNC Server* is listening for download requests, for example `http://192.168.2.187:5800`.

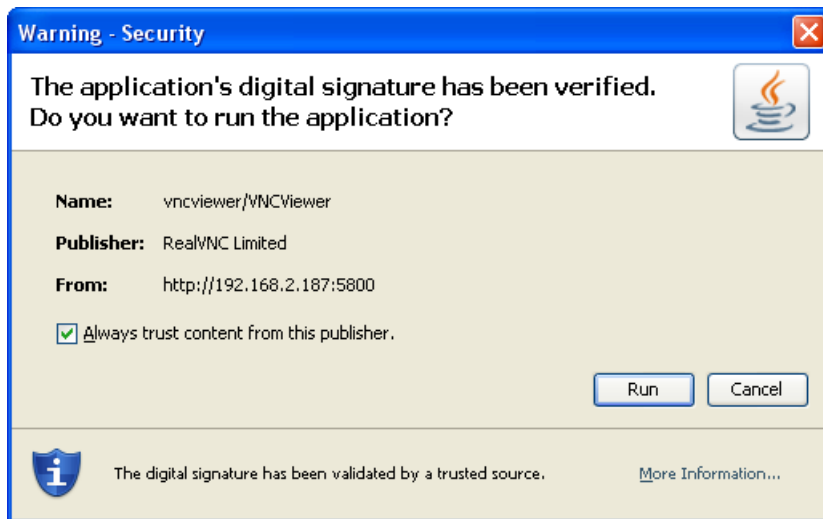
If you do not know a network address for the host computer and you do not have access to it, you will need to consult your system administrator or a host computer user. If you *do* have access to the host computer, follow the instructions in *Step 2: Start VNC Viewer on the client computer* on page 17. Note that if you are connecting over a private network, the information you need is displayed in the **VNC Server Status** dialog, marked **URL**:



If you are connecting over the Internet, you will probably need to enter the network address of a router instead.

By default, *VNC Server* listens for download requests on port 5800. If the download request fails, it may be because *VNC Server* is listening on a different port; see *Qualifying a network address with a port number* on page 24 for relevant information. A download request may also fail if the host computer is protected by a router and/or a firewall and these devices have not been configured to allow access to *VNC Server* at the correct port. For more information on this, and connection issues in general, see *Troubleshooting connection* on page 21.

3. If this is the first time you have used *VNC Viewer for Java*, you may be prompted to trust it:

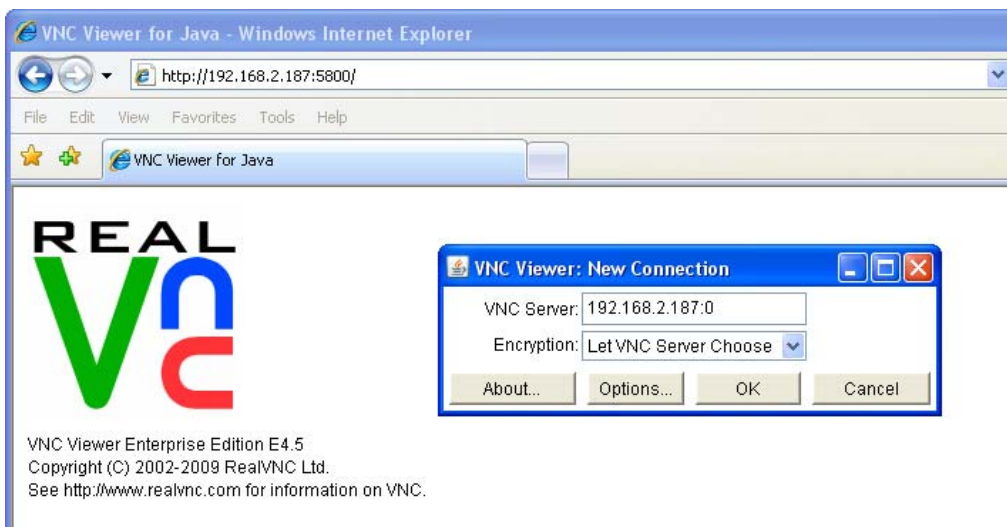


(Windows XP)

You can do this in complete confidence. However, you can choose *not* to trust *VNC Viewer for Java* and still connect, though note you cannot copy and paste text between applications running on the client and host computers in the normal way.

In the example above, click the **Run** button to trust *VNC Viewer for Java*, and **Cancel** to continue connecting without trusting it.

If *VNC Viewer for Java* successfully downloads, the **VNC Viewer: New Connection** dialog opens:



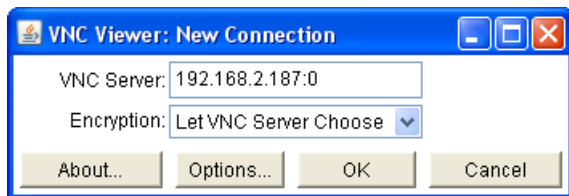
(Windows XP. The web browser is Internet Explorer 7)

Note that the web browser window must stay open while the connection is in progress.

Connecting to VNC Server

The second stage is to use *VNC Viewer for Java* to connect to *VNC Server*. This is the same as connecting from *VNC Viewer*.

By default, the **VNC Server** dropdown on the **VNC Viewer: New Connection** dialog displays the network address of the host computer from which *VNC Viewer for Java* was downloaded, qualified by the port number on which *VNC Server* is listening for connection requests (in the example below, the digit 0 corresponds to the default port, 5900):



(Windows XP)

For more information on network addresses and port numbers, see *Step 3: Identify VNC Server on the host computer* on page 17.

Note: Providing you chose to trust *VNC Viewer for Java* when you downloaded it, you can connect to a *different* host computer. Enter a valid network address in the **VNC Server** dropdown, qualified, if applicable, by the port number on which *VNC Server* is listening for connection requests.

To continue connecting:

1. From the **Encryption** dropdown, select an encryption option, or retain the default: `Let VNC Server choose`. For more information on this, see *Step 4: Select an encryption option* on page 19.
2. If you want to configure *VNC Viewer for Java* before you connect, click the **Options** button. For information on why you might want to do this, see *Configuring VNC Viewer for Java before you connect* on page 53.
3. Click the **OK** button.

You may be asked to confirm a signature that uniquely identifies *VNC Server*, and to authenticate yourself. For more information on these issues, see *Step 5: Connect and authenticate to VNC Server* on page 19.

If the connection is successful, *VNC Viewer for Java* displays the host computer's desktop in a new window on the client computer. Carry on from *Connected: The VNC Viewer for Java experience* on page 54.

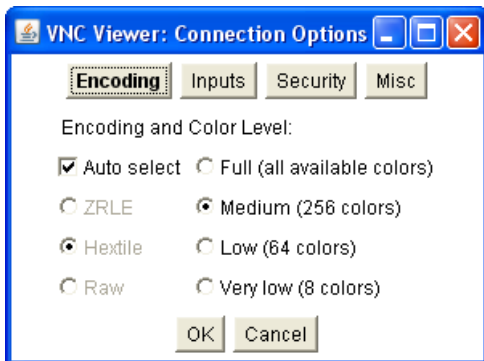
If the connection fails for any reason, start with *Troubleshooting connection* on page 21.

Configuring VNC Viewer for Java before you connect

VNC Viewer for Java is ready to connect to *VNC Server* and control a host computer out-of-the-box. You do not need to configure it. However, you can change some aspects to suit your requirements and environment if you wish.

Some properties must be configured before you connect. Most, however, can be configured once you are connected, and changes applied to the current connection. For more information, see *Using the VNC Viewer for Java Connection Options dialog* on page 56.

To configure *VNC Viewer for Java* before you connect, click the **Options** button in the **VNC Viewer: New Connection** dialog. The **VNC Viewer: Connection Options** dialog opens:



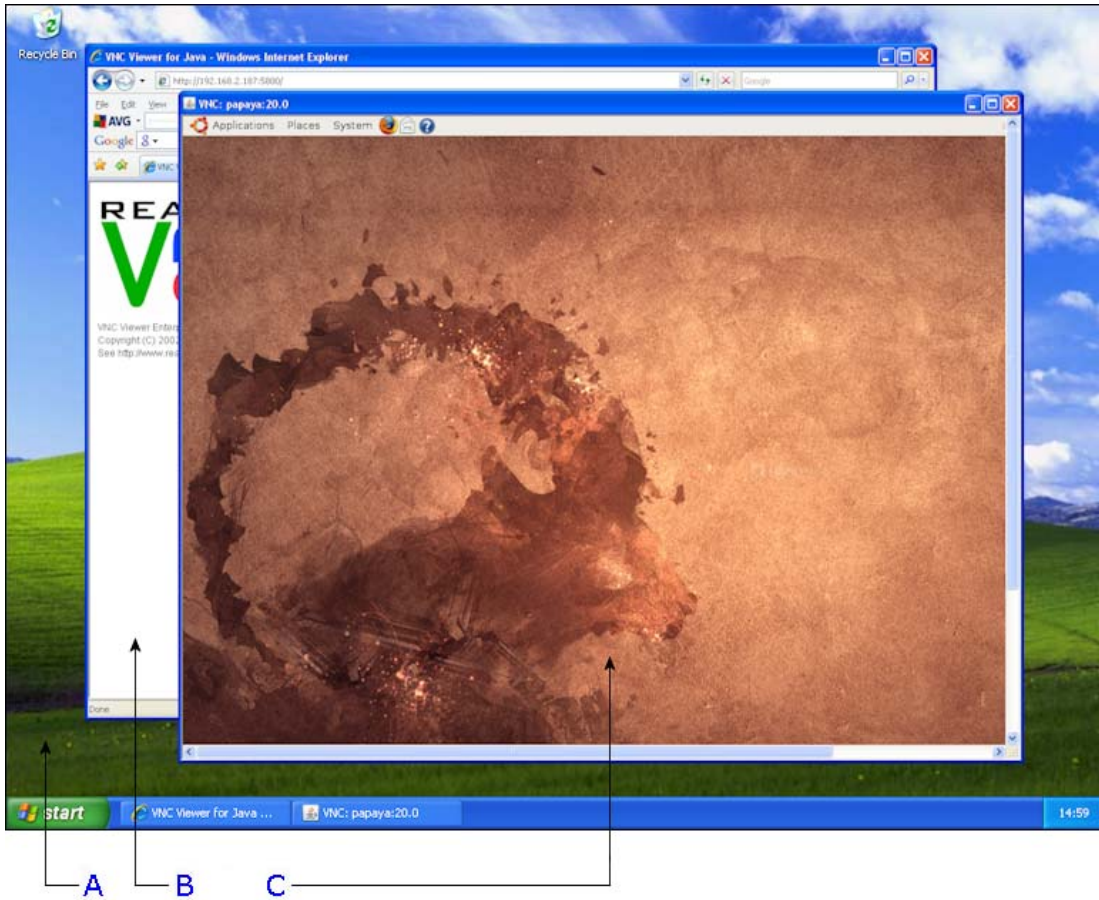
(Windows XP)

The following properties must be configured before a connection is made:

- To make the connection more secure, choose an alternative to the default key length of **512 bits**. This property is on the **Security** tab.
- To ensure your privacy at the start of the connection, turn off **Shared (don't disconnect other VNC Viewers)** in order to disconnect other users. This property is on the **Misc** tab.

Connected: The VNC Viewer for Java experience

When a connection is established, *VNC Viewer for Java* displays the host computer's desktop in a new window on the client computer:



A. Desktop of a client computer running Windows XP. **B.** Java-enabled web browser. This window must stay open while the connection is in progress. **C.** VNC Viewer for Java displaying the desktop of a host computer running Ubuntu 8.10 Linux.

The client computer's keyboard and mouse are now shared with the host computer in exactly the same way as VNC Viewer. For more information, see *Controlling the host computer using your keyboard and mouse* on page 37.

Working with VNC Viewer for Java

You can use *VNC Viewer for Java* to:

- Control the host computer using your keyboard and mouse.
- Copy and paste text between applications running on the client and host computers.
- Trade performance for picture quality while the connection is in progress.
- Restrict access to functionality while the connection is in progress.

See the sections below for more information on these issues. For a summary of functionality that is *not* available, see *Connecting from a web browser* on page 13.

Using the VNC Viewer for Java shortcut menu

VNC Viewer for Java has a shortcut menu to facilitate common operations.

Note: *VNC Viewer for Java* does not have a toolbar.

To open the shortcut menu, press the F8 key (you may need to hold down the FN key under Mac OS X):

| |
|---------------------|
| Exit VNC Viewer |
| Clipboard... |
| Send F8 |
| Send Ctrl-Alt-Del |
| Refresh screen |
| New connection... |
| Options... |
| Connection info... |
| About VNC Viewer... |
| Dismiss menu |

(Windows XP)

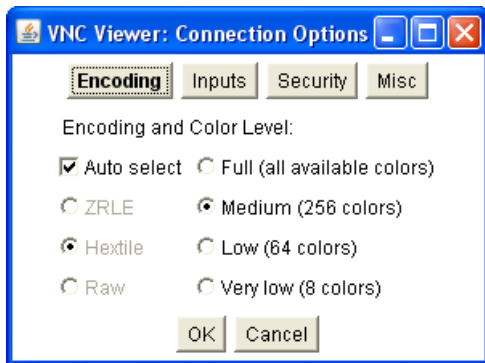
The following table explains the effect of selecting these menu options.

| Shortcut menu option | Explanation |
|----------------------|--|
| Exit VNC Viewer | Closes <i>VNC Viewer for Java</i> . |
| Clipboard | Opens the VNC clipboard dialog. You can preview the contents of the Clipboard and, providing copy and paste is enabled, paste it to an application running either on the client or on the host computer. For more information, see <i>Copying and pasting</i> on page 57. Note that if you chose not to trust <i>VNC Viewer for Java</i> when you downloaded it, you can only copy and paste text between the two computers via this dialog. |
| Send F8 | Sends an F8 command to the host computer. (F8 opens the shortcut menu.) |

| Shortcut menu option | Explanation |
|----------------------|--|
| Send Ctrl-Alt-Del | Sends the CTRL-ALT-DELETE command to the host computer. (Pressing this key combination would be interpreted by the client computer.) |
| Refresh screen | Refreshes the display of the host computer's desktop. |
| New connection | Opens the VNC Viewer: New Connection dialog. You can start a new connection to the same host computer, or to a different one, using the same web browser session. You do not need to download <i>VNC Viewer for Java</i> again. For more information, see <i>Connecting to VNC Server</i> on page 52. |
| Options | Opens the VNC Viewer: Connection Options dialog. You can configure most aspects of <i>VNC Viewer for Java</i> while the current connection is in progress. For more information, see <i>Using the VNC Viewer for Java Connection Options dialog</i> on page 56. Note that some properties must be configured before you connect. For more information, see <i>Configuring VNC Viewer for Java before you connect</i> on page 53. |
| Connection info | Opens a dialog displaying technical information about the current connection, such as the encryption method and compression format. |
| About VNC Viewer | Displays information about <i>VNC Viewer for Java</i> . |
| Dismiss menu | Closes the shortcut menu. |

Using the VNC Viewer for Java Connection Options dialog

The **VNC Viewer: Connection Options** dialog enables you to configure *VNC Viewer for Java* while the current connection is in progress:



(Windows XP)

Note: Some *VNC Viewer for Java* properties must be configured *before* you connect. For more information, see *Configuring VNC Viewer for Java before you connect* on page 53.

To open the **VNC Viewer: Connection Options** dialog, select **Options** from the shortcut menu. For more information on this menu, see *Using the VNC Viewer for Java shortcut menu* on page 55.

The following sections explain the properties in this dialog.

Trading performance for picture quality

You may be able to enhance the performance of *VNC Viewer for Java* by reducing the number of colors used to display the host computer's desktop. To do this, turn off **Auto Select** and choose either 256, 64, or 8 colors. These properties are on the **Encoding** tab.

You can also choose an alternative to the default **ZRLE** encoding. The **Hextile** and **Raw** encodings require increasingly less processing power to display the host computer's desktop, though note they also require progressively more bandwidth.

Restricting access to functionality

You can quickly prevent all interchange with the host computer, making *VNC Viewer for Java* 'view only'. To do this, turn on **View only (ignore mouse & keyboard)**. This property is on the **Inputs** tab.

You can disable copy and paste, or just copy and paste in a particular direction. For more information, see *Copying and pasting* on page 57.

Troubleshooting display

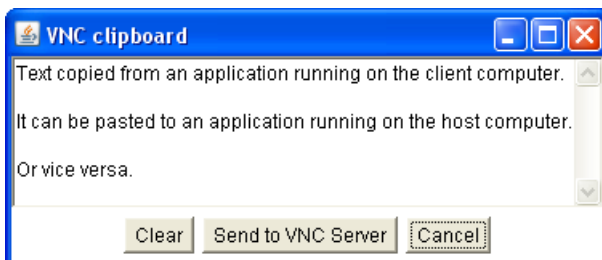
If the mouse cursor is not behaving in the expected way, turn off **Render cursor locally**. This property is on the **Misc** tab.

If the screen is not updating properly, turn off **Fast CopyRect**. This property is on the **Misc** tab.

Copying and pasting

You can copy and paste text between applications running on the client and host computers. This feature works in the same way as it does for *VNC Viewer*. Follow the instructions in *Copying and pasting text between client and host computers* on page 66.

You can preview the contents of the Clipboard to see what text is available to paste. To do this, open the shortcut menu and select **Clipboard**. For more information on this menu, see *Using the VNC Viewer for Java shortcut menu* on page 55. The **VNC clipboard** dialog opens:



(Windows XP)

Disabling and enabling copy and paste

You can disable copy and paste while the current connection is in progress. To do this, open the **VNC Viewer: Connection Options** dialog. For more information on this dialog, see *Using the VNC Viewer for Java Connection Options dialog* on page 56. On the **Inputs** tab, turn off **Accept clipboard from VNC Server** and **Send clipboard to VNC Server**.

Chapter 4: Connecting From A Web Browser

Note you can turn these properties off separately in order to disable copy and paste in one direction only.

5

Exchanging Information

This chapter explains how to use *VNC Viewer* to exchange information with the host computer, or with other users connected at the same time as you.

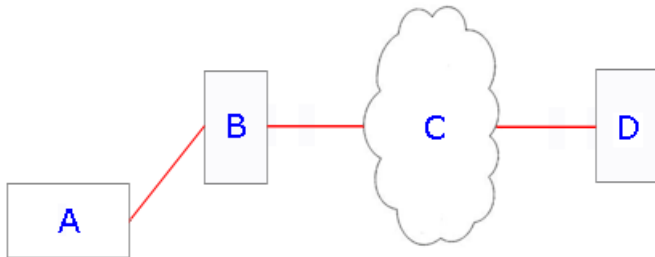
Note: This chapter assumes you are connected to a host computer using fully-featured *VNC Viewer*. If not, some or all of these features may be unavailable. For more information, see *VNC Enterprise Edition 4.5 connectivity* on page 12.

Contents

| | |
|--|----|
| Printing host computer files to a local printer | 60 |
| Transferring files between client and host computers | 62 |
| Copying and pasting text between client and host computers | 66 |
| Communicating securely using VNC Chat | 67 |

Printing host computer files to a local printer

You can print host computer files directly to the default printer attached to the client computer (that is, to a *local* printer).



A. Local printer. **B.** Client computer running VNC Viewer. Printer (A) must be set as the client's default printer. **C.** A network, for example the Internet. **D.** Host computer running VNC Server.

Note: To see how to make a printer the client computer's default, consult its operating system documentation.

This powerful feature is ready to use out-of-the-box. Open a host computer file in the *VNC Viewer* window and print in the expected way for the application, for example by selecting **File > Print**. The local printer is automatically shared with the host computer and made *its* default while the connection is in progress, so the correct device should already be selected. Your request is added to the local printer's queue and executed in turn.

VNC Enterprise Edition attempts a best possible quality print finish. This may mean the contents of the file are scaled to fit the dimensions of the local printer's paper. If the results are unexpected, see *Manipulating the quality of the print finish* on page 60.

If the host computer file does not print to the local printer, start with *Troubleshooting printing* on page 61.

Disabling and enabling printing

You can disable printing providing you do so before you connect. Open the **VNC Viewer Properties** dialog and, on the **Printing** tab, choose **Don't share a printer**. For more information, see *Configuring printing* on page 34. Note that you can enable printing again for future connections at any time.

You can still print but choose not to change the host computer's default printer. To do this, turn off **Make it the default printer on VNC Server**. This means you will have to explicitly select the local printer when you print. The local printer has a name of the form <printer name> via VNC from <client computer name>, for example HP LaserJet via VNC from Neptune.

Manipulating the quality of the print finish

The quality of the print finish is determined by the characteristics of the local printer. For example, if the host computer file is a color photo but the local printer only prints in black and white, then color will be lost.

You may be able to configure printer properties in order to achieve a better quality print finish. You should do this before you connect in the way expected for the operating system of the client computer, for example by selecting **Control Panel > Printers and Faxes** under Windows XP.

If you are already connected, then you may be able to configure some printing preferences for the application you are printing from. This may include rotating pages, changing the page order, choosing a number of pages per sheet, and advanced options such as changing the resolution or paper size. For more information, consult the application's documentation.

Troubleshooting printing

Printing host computer files to a local printer should work out-of-the-box. If it does not, check the following:

1. Are both client and host computers running version 4.5 of *VNC Viewer* and *VNC Server* respectively? Printing is not supported by earlier versions.
2. Make sure the local printer is connected to the client computer, that it is switched on and ready to print (for example, it has paper), and that it is set as the client computer's default printer.
3. *VNC Viewer* may have been configured to disable printing. To see how to enable it again, read *Disabling and enabling printing* on page 60. You will have to close the current connection and then reconnect.
4. *VNC Viewer* may have been configured to prevent the local printer becoming the host computer's default, which means the local printer is not automatically selected. The request may have been sent to the wrong printer. To see how to make the local printer the host computer's default so it is always selected, read *Disabling and enabling printing* on page 60. You will have to close the current connection and then reconnect.

Note that if another *VNC Viewer* user connected to the same host computer before you, then *their* local printer becomes the host computer's default. You cannot change this. You will always have to explicitly select your local printer when you print.

If you have to explicitly select the local printer, it will have a name of the form `<printer name> via VNC from <client computer name>`, for example `HP LaserJet via VNC from Neptune`.

5. *VNC Server* may have been configured to prevent printing. If this is the case and you do not have access to the host computer, you will need to consult your system administrator or a host computer user. If you *do* have access to the host computer, and sufficient privileges to configure *VNC Server*, you may be able to allow it again. For more information, see *Preventing printing* on page 91.
6. *VNC Server* may have been configured to prevent *you* printing. If this is the case and you do not have access to the host computer, you will need to consult your system administrator or a host computer user. If you *do* have access to the host computer, and sufficient privileges to configure *VNC Server*, you may be able to allow it again. Alternatively, you may be able to connect as a different host computer user and access this functionality. For more information, see *Restricting functionality for particular connected users* on page 110.
7. The host computer itself may have been configured to prevent printing system-wide. If this is the case and you do not have access to the host computer, you will need to consult your system administrator or a host computer user. If you *do* have access to the host computer, and sufficient privileges to configure both it and *VNC Server*, you may be able to allow it again. For more information, see *Preventing printing* on page 91.
8. If the host computer is running Linux or Mac OS X, CUPS version 1.3 or later must be installed. If you have access to the host computer, consult the operating system documentation.

Transferring files between client and host computers

You can exchange files with the host computer.



This section explains the *VNC Enterprise Edition* file transfer mechanism. You should use this mechanism to exchange files in all circumstances *except* when the host computer is running Windows and *VNC Server* is in Service Mode, in which case you can copy and paste files in the standard way for Windows. Follow the appropriate instructions for the platform of the *host* computer below.

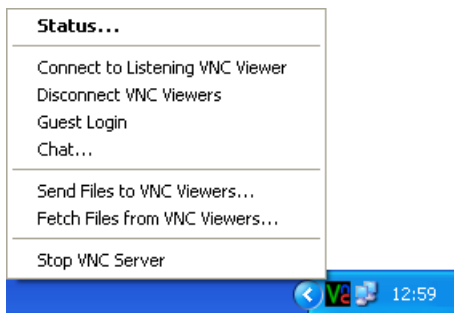
Note: For more information on *VNC Server* in Service Mode, see *Running multiple instances of VNC Server* on page 76.

If transferring files fails for any reason, start with *Troubleshooting file transfer* on page 65.

Windows

To send client computer files to a host computer running Windows:

1. Click the **Send Files To VNC Server**  *VNC Viewer* toolbar button. A standard file selection dialog opens.
2. Select one or more files, or an entire folder, to send to the host computer, and confirm the operation. The files are now ready to send.
3. For *VNC Server* in User Mode, right-click the *VNC Server* icon  in the host computer's Notification area (shaded black). The *VNC Server* shortcut menu opens. Carry on from step 4.





(Windows XP)

For *VNC Server* in Service Mode, paste the file(s) to a location on the host computer in the standard way, for example by pressing CTRL-V. You do not need to perform steps 4 and 5.


4. Select **Fetch Files from VNC Viewers**. The standard Windows browse folder dialog opens.
5. Choose a location on the host computer to transfer the file(s) to, and confirm the operation to proceed.

To fetch files from a host computer running Windows:

1. For *VNC Server* in User Mode, right-click the *VNC Server* icon  in the host computer's Notification area (shaded black). The *VNC Server* shortcut menu opens (see example above). Carry on from step 2.
For *VNC Server* in Service Mode, copy the file(s) in the standard way, for example by pressing CTRL-C, and then click the **Fetch Files From VNC Server**  *VNC Viewer* toolbar button. A download location dialog opens. Carry on from step 4.
2. Select **Send Files to VNC Viewers**. The standard Windows open file dialog opens.
3. Select one or more files, or click the **Use Entire Folder** button. A download location dialog opens.
4. Choose a location on the client computer to transfer the file(s) to, and confirm the operation to proceed.

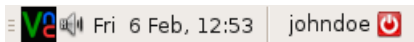
UNIX or Linux

To send client computer files to a host computer running UNIX or Linux:

1. Click the **Send Files To VNC Server**  *VNC Viewer* toolbar button. A file selection dialog opens.
2. Select one or more files, or an entire folder, to send to the host computer, and confirm the operation. The **Fetch Files** dialog opens.
3. Choose a location on the host computer to transfer the file(s) to, and click the **OK** button.

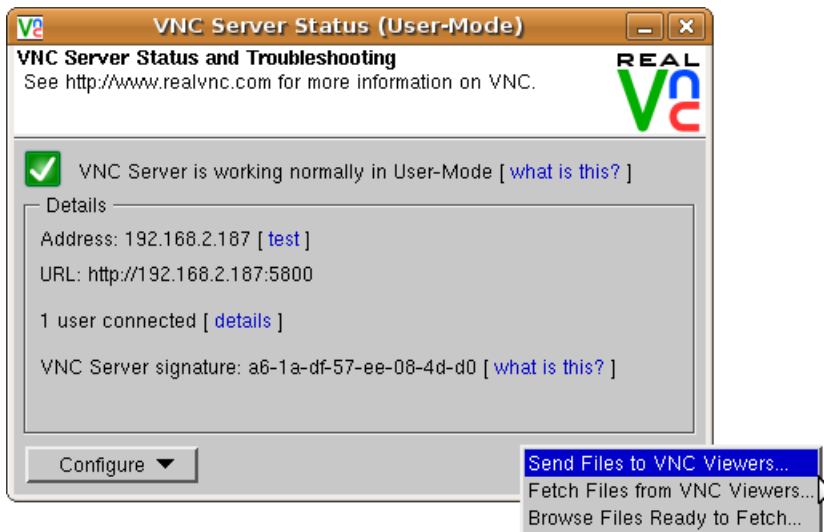
To fetch files from a host computer running UNIX or Linux:

1. Click the *VNC Server* icon  in the host computer's Notification Area (which may be shaded black):



The **VNC Server Status** dialog opens. If no *VNC Server* icon is displayed, see *Troubleshooting file transfer* on page 65.

2. Click the **Files** button to open a menu, and select **Send Files to VNC Viewers:**




(Ubuntu 8.10 Linux)

The **Share Files** dialog opens.


3. Select a file, or an entire folder, and click the **OK** button. A download location dialog opens.
4. Choose a location on the client computer to transfer the file(s) to, and confirm the operation to proceed.

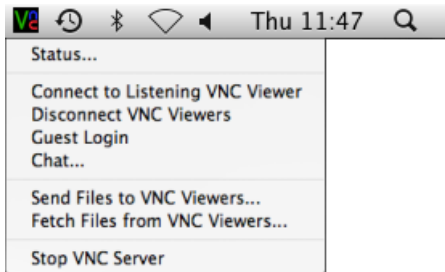
Mac OS X

To send client computer files to a host computer running Mac OS X:

1. Click the **Send Files To VNC Server**  **VNC Viewer** toolbar button. A file selection dialog opens.
2. Select one or more files, or an entire folder, to send to the host computer, and confirm the operation. The **Select directory to save fetched files** dialog opens.
3. Choose a location on the host computer to transfer the file(s) to, and click the **Save** button.

To fetch files from a host computer running Mac OS X:

1. Click the *VNC Server* icon  in the host computer's Status bar (shaded black). The *VNC Server* shortcut menu opens:



(Mac OS X 10.5)

2. Select **Send Files to VNC Viewers**. The **Select files or directory to share** dialog opens.
3. Select one or more files, or an entire folder, and click the **Share** button. A download location dialog opens.
4. Choose a location on the client computer to transfer the file(s) to, and confirm the operation to proceed.

Disabling and enabling file transfer

You can disable file transfer while the current connection is in progress.

To do this, open the **VNC Viewer Properties** dialog and, on the **Inputs** tab, turn off **Enable file transfer**. For more information on this dialog, see *Using the VNC Viewer Properties dialog* on page 41. The **Send Files**

To VNC Server  *VNC Viewer* toolbar button is disabled.


You can enable file transfer again at any time.

Troubleshooting file transfer

If file transfer does not work, check the following:

1. *VNC Viewer* may have been configured to disable file transfer. To see how to enable it again, read *Disabling and enabling file transfer* on page 65.
2. *VNC Server* may have been configured to prevent file transfer. If this is the case and you do not have access to the host computer, you will need to consult your system administrator or a host computer user. If you *do* have access to the host computer, and sufficient privileges to configure *VNC Server*, you may be able to allow it again. For more information, see *Preventing file transfer* on page 91.
3. *VNC Server* may have been configured to prevent *you* transferring files. If this is the case and you do not have access to the host computer, you will need to consult your system administrator or a host computer user. If you *do* have access to the host computer, and sufficient privileges to configure *VNC Server*, you may be able to allow it again. Alternatively, you may be able to connect as a different host computer user and access this functionality. For more information, see *Restricting functionality for particular connected users* on page 110.

4. Under UNIX or Linux, for *VNC Server* in Virtual Mode, a program called `vnconfig` may not be running.

If this is the case, no *VNC Server* icon  is displayed in the Notification Area, and file transfer is disabled. To enable it again, type `vnconfig` in a Terminal window, and press the ENTER key.

Note that under some versions of UNIX, a *VNC Server* icon is never available. However, file transfer may still be enabled in this case.

Copying and pasting text between client and host computers

You can copy and paste text between applications running on the client and host computers.

Note that, when pasted, any formatting applied to the copied text is lost, and that the computer you are pasting to must support the language of the copied text in order for it to be pasted meaningfully.

To copy and paste text from an application on the client computer to one on the host:

1. On the client computer, copy the text in the expected way for the platform of the client computer, for example by selecting it and pressing `Ctrl-C` (`Cmd-C` on Mac OS X). The text is copied to the Clipboard.
2. Give the *VNC Viewer* window focus, open the destination application on the host computer, and paste the text in the expected way for the host's platform, for example by pressing `Ctrl-V`. (To emulate `Cmd-V` on a Mac OS X host, press `Alt-V` on a PC keyboard.)

To copy and paste text from an application on the host computer to one on the client:

1. Within the *VNC Viewer* window, copy the text in the expected way for the platform of the host computer, for example by selecting it and pressing `Ctrl-C`. (To emulate `Cmd-C` on a Mac OS X host, press `Alt-C` on a PC keyboard.) The text is copied to the Clipboard.
2. Give the destination application on the client computer focus, and paste the text in the expected way for the client's platform, for example by pressing `Ctrl-V` (`Cmd-V` on Mac OS X).

If copy and paste fails for any reason, start with *Troubleshooting copy and paste* on page 66.

Disabling and enabling copy and paste

You can disable copy and paste while the current connection is in progress.

To do this, open the **VNC Viewer Properties** dialog and, on the **Inputs** tab, turn off **Share clipboard with VNC Server**. For more information on this dialog, see *Using the VNC Viewer Properties dialog* on page 41.

You can enable copy and paste again at any time.

Troubleshooting copy and paste


If copy and paste does not work, check the following:

1. *VNC Viewer* may have been configured to disable copy and paste. To see how to enable it again, read *Disabling and enabling copy and paste* on page 66.
2. *VNC Server* may have been configured to prevent copy and paste. If this is the case and you do not have access to the host computer, you will need to consult your system administrator or a host computer user.

If you *do* have access to the host computer, and sufficient privileges to configure *VNC Server*, you may be able to allow it again. For more information, see *Preventing copy and paste* on page 91.

3. *VNC Server* may have been configured to prevent *you* copying and pasting. If this is the case and you do not have access to the host computer, you will need to consult your system administrator or a host computer user. If you *do* have access to the host computer, and sufficient privileges to configure *VNC Server*, you may be able to allow it again. Alternatively, you may be able to connect as a different host computer user and access this functionality. For more information, see *Restricting functionality for particular connected users* on page 110.

4. Under UNIX or Linux, for *VNC Server* in Virtual Mode, a program called `vnccfg` may not be running.


If this is the case, no *VNC Server* icon  is displayed in the Notification Area, and copy and paste is disabled. To enable it again, type `vnccfg` in a Terminal window, and press the ENTER key.

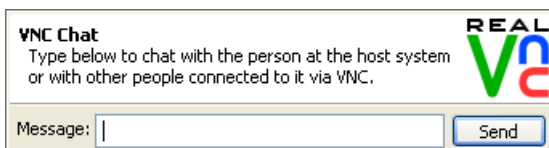
Note that under some versions of UNIX, a *VNC Server* icon is never available. However, copy and paste may still be enabled in this case.

Communicating securely using VNC Chat

You can chat with other *VNC Viewer* users connected to a host computer at the same time as you, and also with a host computer user if one is present.

Note: You cannot chat with connected web browser users.

To participate in a conversation, or start a new one, click the **Start Chat Session**  *VNC Viewer* toolbar button. A message box appears at the bottom of the *VNC Viewer* window:



(Windows XP)

Enter a message and click the **Send** button. The message is broadcast to a conversation window on the host computer visible to you and to all other connected users (including a host computer user, if present):



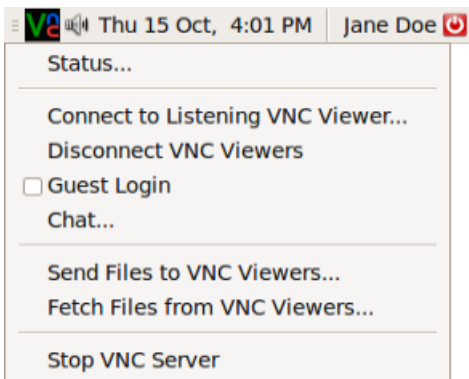
(Ubuntu 9.04 Linux)

Note: You are identified by the user name with which you authenticated to *VNC Server*, or as *VNC Viewer* if you did not enter a user name to connect.

Using VNC Chat as a host computer user

A host computer user can participate in a conversation, or start a new one. To start a new conversation as a host computer user:

1. Open the *VNC Server* shortcut menu. For more on this menu, see *Using the VNC Server shortcut menu* on page 80.

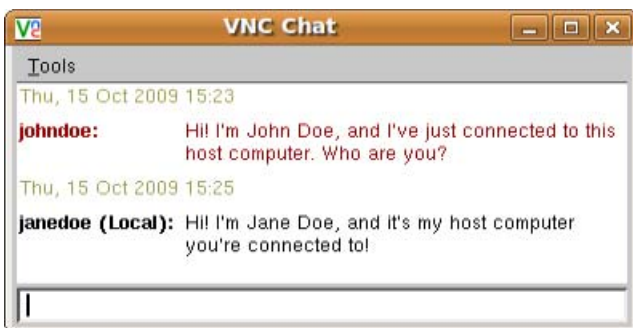


(Ubuntu 9.04 Linux)

2. Select **Chat**. The conversation window opens. Type text in the field at the bottom:



3. Press the ENTER key to send the message:

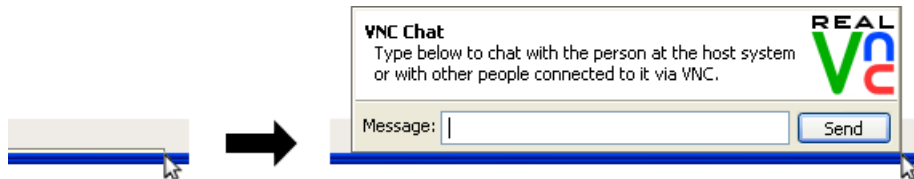


(Ubuntu 9.04 Linux)

Note: A host computer user is identified by the text `(Local)` appended to the user name.

Working with VNC Chat

In *VNC Viewer*, the message box is minimized when *VNC Chat* is not being used. To see it again, hover the mouse over the hot area at the bottom of the *VNC Viewer* window:



(Windows XP)

By default, messages are stored on the host computer for 90 days. To stop recording messages, select **Tools > Options** in the conversation window and turn off **Log chat history**. Alternatively, you can reduce the number of days, or switch to storing a particular number of messages.

If you stop recording and also want to clear the conversation window, you must delete the `vncchat.xml` file. Under UNIX or Linux and Mac OS X, this file is located in the host computer user's `.vnc` directory (you can configure the location under Windows). Under UNIX or Linux and Mac OS X, you must then stop and restart *VNC Server*.

Note that when a *VNC Viewer* user disconnects, messages sent by that user turn gray in the conversation window.

Disabling and enabling VNC Chat

You can disable *VNC Chat* while the current connection is in progress.

To do this, open the **VNC Viewer Properties** dialog and, on the **Inputs** tab, turn off **Enable chat**. For more information on this dialog, see *Using the VNC Viewer Properties dialog* on page 41. The **Start Chat**

Session 🗨️ *VNC Viewer* toolbar button is disabled.

Note: *VNC Chat* is only disabled for you, and not for any other connected *VNC Viewer* user. You can still view messages in the host computer conversation window.

You can enable *VNC Chat* again at any time.

Troubleshooting VNC Chat

If you cannot use *VNC Chat*, check the following:

1. Is there anyone to chat with? The **VNC Server Status** dialog lists connected *VNC Viewer* users:

2 users connected [[details](#)]

For more information on this dialog, see *Using the VNC Server Status dialog* on page 81.

2. *VNC Viewer* may have been configured to disable *VNC Chat*. To see how to enable it again, read *Disabling and enabling VNC Chat* on page 69.
3. *VNC Server* may have been configured to prevent chat. If this is the case and you do not have access to the host computer, you will need to consult your system administrator or a host computer user. If you *do*

have access to the host computer, and sufficient privileges to configure *VNC Server*, you may be able to allow it again. For more information, see *Preventing chat* on page 91.

4. *VNC Server* may have been configured to prevent *you* chatting. If this is the case and you do not have access to the host computer, you will need to consult your system administrator or a host computer user. If you *do* have access to the host computer, and sufficient privileges to configure *VNC Server*, you may be able to allow it again. Alternatively, you may be able to connect as a different host computer user and access this functionality. For more information, see *Restricting functionality for particular connected users* on page 110.

6

Setting Up VNC Server

VNC Server permits encrypted, authenticated connections to the host computer on which it runs out-of-the-box. You should not need to configure it. However, you can change almost any aspect to suit your requirements and environment if you wish.

This chapter explains how to work with *VNC Server*. It also explains advanced scenarios such as running multiple instances concurrently, configuring network communications, and restricting access to functionality for connected users. This chapter assumes you have access to the host computer and sufficient privileges to configure both it and *VNC Server*. If you are setting up *VNC Server* on your own computer for remote access, note that some features require a user to be present at the host computer in order to work.

Note: For more information on security, see *Chapter 7, Security* on page 93.

Contents

| | |
|---|----|
| Starting VNC Server | 72 |
| Running multiple instances of VNC Server | 76 |
| Working with VNC Server | 79 |
| Configuring network communications | 86 |
| Preventing connections to VNC Server | 88 |
| Restricting functionality for connected users | 90 |
| Stopping VNC Server | 92 |

Starting VNC Server

To start *VNC Server*, follow the appropriate instructions for the host computer's platform below.

Note: As soon as *VNC Server* starts, users can connect. To delay or prevent connections, see *Preventing connections to VNC Server* on page 88.

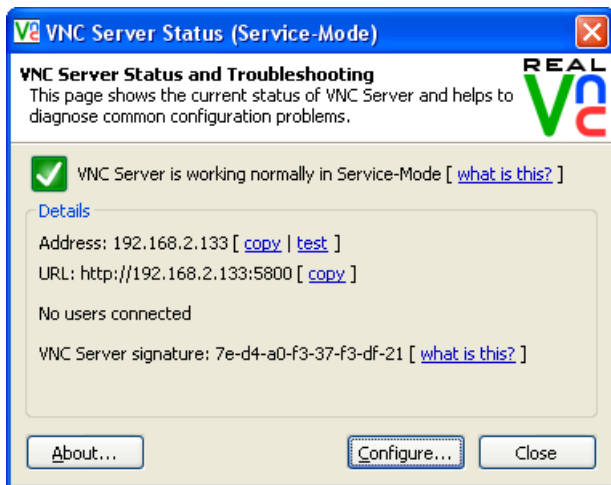
Windows

VNC Server can start in Service Mode, in User Mode, or both. For more information on these modes, which you might want to use, and why you might want to run more than one instance of *VNC Server*, see *Running multiple instances of VNC Server* on page 76.

To start *VNC Server*:


- In Service Mode, select **RealVNC > VNC Server** from the **Start** menu. You may be required to confirm this operation. Note that, by default, *VNC Server* starts in this mode automatically when the computer is powered on. To see how to prevent this, read *Preventing VNC Server starting automatically (Windows only)* on page 75.
- In User Mode, select **RealVNC > Advanced > VNC Server (User Mode)** from the **Start** menu.

The **VNC Server Status** dialog opens:



(Windows XP. In this example, *VNC Server* is in Service Mode.)

The **VNC Server Status** dialog is the gateway to *VNC Server* and all its operations. For more information, see *Using the VNC Server Status dialog* on page 81.

Click the **Close** button to minimize the **VNC Server Status** dialog but keep *VNC Server* running in the background. To access the dialog again, double-click the *VNC Server* icon  in the Notification area. For more information, see *Using the VNC Server icon* on page 79.

To see how to stop *VNC Server*, or to learn why *VNC Server* might stop automatically, read *Stopping VNC Server* on page 92.

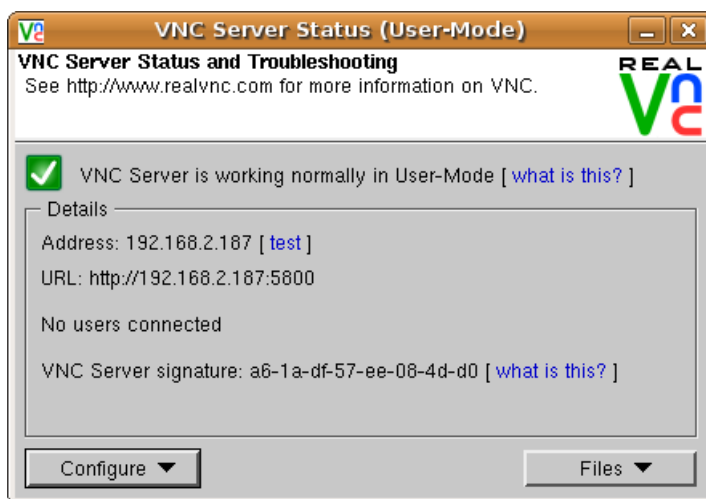
UNIX or Linux

VNC Server can start in User Mode, in Virtual Mode, or both. In addition, VNC Server can start in Virtual Mode as many times as your license permits. For more information on these modes, which you might want to use, and why you might want to run more than one instance of VNC Server, see *Running multiple instances of VNC Server* on page 76.

To start VNC Server:



- In User Mode, either:
 - Type `x0vncserver` in a Terminal window, and press the ENTER key.
 - Select **Applications > Internet > VNC Server (User Mode)** from the menu system, if available.

The **VNC Server Status** dialog opens:



(Ubuntu 8.10 Linux)

The **VNC Server Status** dialog is the gateway to VNC Server in User Mode and all its operations. For more information, see *Using the VNC Server Status dialog* on page 81.

Under most versions of UNIX and Linux, you can click the dialog's **Close** button  to minimize the **VNC Server Status** dialog but keep VNC Server in User Mode running in the background. To access the dialog again, click the VNC Server icon  in the Notification Area. See *Using the VNC Server icon* on page 79 for more information.

Note: Under some versions of UNIX, a VNC Server icon is not available. In these circumstances, clicking the **Close** button stops VNC Server.

- In Virtual Mode, type `vncserver` in a Terminal window, and press the ENTER key. A message ending with text similar to the following appears:

```
New desktop is johndoe:1 (192.168.2.187:1)
```

This operation starts *VNC Server* in Virtual Mode attached to a *virtual* desktop, detached from the monitor, and independent of the console. This means that no *VNC Server* icon and **VNC Server Status** dialog comparable to that of *VNC Server* in User Mode can be displayed. To see how to work with *VNC Server* in Virtual Mode, read *Working with VNC Server in Virtual Mode (UNIX or Linux only)* on page 75.

A virtual desktop is assigned an X Server session number corresponding to the port on which *VNC Server* is listening for connection requests. In the example above, this is X Server session number 1, corresponding to port 5901. For more information on ports, see *Configuring network communications* on page 86.


To see how to stop *VNC Server*, or to learn why *VNC Server* might stop automatically, read *Stopping VNC Server* on page 92.

Mac OS X

VNC Server can start in Service Mode, in User Mode, or both. In addition, *VNC Server* can start in User Mode as many times as your license permits. For more information on these modes, which you might want to use, and why you might want to run more than one instance of *VNC Server*, see *Running multiple instances of VNC Server* on page 76.

To start *VNC Server*:

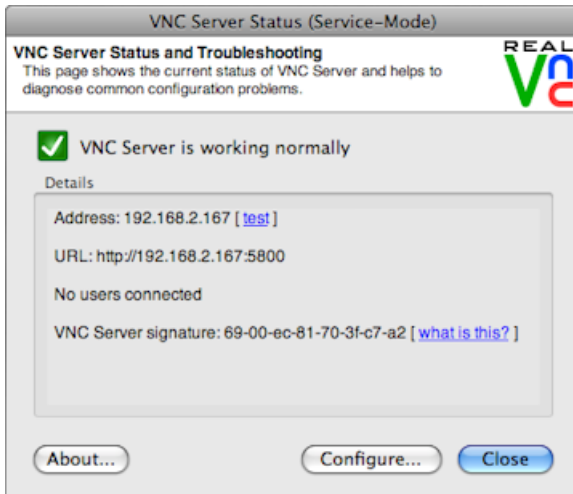
- In Service Mode, navigate to the **Applications > RealVNC** folder, and double-click the **VNC Server** program. You may be required to confirm this operation.
- In User Mode, navigate to the **Applications > RealVNC > Advanced** folder, and double-click the **VNC Server (User Mode)** program.

In either mode, a *VNC Server* icon  appears in the Status bar:



(Mac OS X 10.5)

Click the *VNC Server* icon to open the *VNC Server* shortcut menu, and select the **Status** option. The **VNC Server Status** dialog opens:



(Mac OS X 10.5. In this example, VNC Server is in Service Mode.)

The **VNC Server Status** dialog is the gateway to *VNC Server* and all its operations. For more information, see *Using the VNC Server Status dialog* on page 81.

Click the **Close** button to minimize the **VNC Server Status** dialog but keep *VNC Server* running in the background. To access the dialog again, select **Status** from the *VNC Server* shortcut menu. For more information, see *Using the VNC Server icon* on page 79.

To see how to stop *VNC Server*, or to learn why *VNC Server* might stop automatically, read *Stopping VNC Server* on page 92.

Preventing VNC Server starting automatically (Windows only)

By default, *VNC Server* in Service Mode starts automatically when a Windows host computer is powered on. This means users can connect before a host computer user logs on.

To prevent *VNC Server* in Service Mode starting automatically, open the **VNC Server Properties** dialog and turn off **Start VNC Server automatically with Windows**. For more information on this dialog, see *Using the VNC Server Properties dialog* on page 85.

Working with VNC Server in Virtual Mode (UNIX or Linux only)

VNC Server in Virtual Mode starts unattached to any physical display hardware. This means that desktop artifacts that help you work with *VNC Server*, such as a *VNC Server* icon and **VNC Server Status** dialog, are not available.

To configure *VNC Server* in Virtual Mode, you can instead:

- Specify parameters on start-up.
- Configure *VNC Server* as a connected user.

Note that changes made using either method are lost when *VNC Server* stops.

Specifying parameters on start-up

You can configure *VNC Server* in Virtual Mode on start-up using parameters.

Parameters can be specified in configuration files, in which case they apply to all instances of *VNC Server* in Virtual Mode automatically, or at the command line when a particular instance starts. *VNC Server* reads parameters in the following order:

1. The system configuration file: `/etc/vnc/config`.
2. The configuration file of the user starting *VNC Server*: `$HOME/.vnc/config`.
3. Appended to the `vncserver` command at the command line.


Parameters specified later in this list override duplicates specified earlier.

For a full list of parameters, type `vncserver -list` at the command line. For more information, type `man vncserver`.

Configuring VNC Server as a connected user

You can connect to *VNC Server* in Virtual Mode and configure it as a connected user. When you disconnect, your changes apply to all future connections to this instance of *VNC Server* while it runs.

Note: To see how to use *VNC Viewer* to connect to *VNC Server*, read *Connecting to a host computer* on page 35. You will need to qualify the network address of the host computer with the X Server session number assigned when *VNC Server* starts, for example `192.168.2.187:1`.

Under most versions of UNIX or Linux, when you connect, a *VNC Server* icon  is displayed in the *VNC Viewer* window. For more information on this icon, including how to use it to open the **VNC Server Status** dialog and configure *VNC Server*, start with *Using the VNC Server icon* on page 79.

Note: If another user connects, the *VNC Server* icon is shaded black.

Note that under some versions of UNIX, a *VNC Server* icon is not available. In these circumstances, the **VNC Server Status** dialog should be running as a standalone application.

Running multiple instances of VNC Server

Under any platform, and providing you have a license to do so, you can run more than one instance of *VNC Server* on a host computer.

This powerful feature means you can set up the host computer so users can connect to it in different ways. For example, you could set up one instance of *VNC Server* so that connections to it are optimized for speed, and another so connections are optimized for security. *VNC Server* facilitates this using *modes*, each of which permits a different level of access to the host computer.

Note: To see how to start *VNC Server* in different modes, read *Starting VNC Server* on page 72.

To find out more, read the section appropriate to the platform of the host computer below.

Windows

Under Windows, a host computer user with administrative privileges can start *VNC Server* in Service Mode. This means *VNC Server* runs, and users can connect, irrespective of whether or not a host computer user is currently logged on. By default, connecting users must know the user name and password of a member of the Administrators group in order to connect. In addition, by default, *VNC Server* starts in Service Mode automatically when the host computer is powered on.

In addition, or alternatively, a host computer user can log on and start *VNC Server* in User Mode. This means *VNC Server* runs, and users can connect, just while this host computer user is logged on. (Connections are terminated on log off.) By default, connecting users must know either the user name and password of the currently logged on host computer user or of a member of the Administrators group in order to connect.

Once connected to *VNC Server* in either mode, a connected user has the same privileges (that is, access rights) on the host computer as the *currently logged on host computer user*. For more information, see *Authenticating connections to VNC Server* on page 94.

Because only one host computer user can log on to a Windows computer at a time, this means a maximum of two instances of *VNC Server* can run concurrently on a Windows host computer – one in Service Mode, and one in User Mode for the currently logged on host computer user. Both instances must listen on different ports; see *Configuring network communications* on page 86 for more information.

UNIX or Linux

Under UNIX or Linux, a host computer user can log on and start *VNC Server* in User Mode. In this mode, *VNC Server* runs attached to the console X Server session, which means that:

- A *VNC Server* icon and **VNC Server Status** dialog can be displayed in order to help the host computer user configure *VNC Server* after it has started, if necessary.
- Connected users can access applications currently running on the host computer.
- *VNC Server* stops, and all connections are terminated, when the host computer user starting *VNC Server* logs off.
- By default, users must know the user name and password of the host computer user starting *VNC Server* in order to connect. Once connected, they have the same privileges (that is, access rights) as this host computer user. For more information on privileges, see *Authenticating connections to VNC Server* on page 94.

Depending on the terms of the license, a host computer user can also, or alternatively, log on and start *VNC Server* in Virtual Mode. In this mode, *VNC Server* runs attached to a new *virtual* desktop, detached from the monitor and independent of the console, which means that:

- No *VNC Server* icon or **VNC Server Status** dialog can be displayed in order to help the host computer user configure *VNC Server* after it has started. To see how to work with *VNC Server* in this mode, read *Working with VNC Server in Virtual Mode (UNIX or Linux only)* on page 75.
- Connected users cannot access applications currently running on the console of the host computer. Instead, an isolated workspace is provided. Note this powerful feature can help prevent conflicts; each user can be directed to connect to their own instance of *VNC Server* in Virtual Mode, and control a (virtual) desktop independently.
- *VNC Server* does not stop when the host computer user logs off. Connected users stay connected, and new users can connect. *VNC Server* must be explicitly stopped.

- By default, users must know the user name and password of the host computer user starting *VNC Server* in order to connect. Once connected, they have the same privileges (that is, access rights) as this host computer user. For more information on privileges, see *Authenticating connections to VNC Server* on page 94.

Under UNIX or Linux, more than one host computer user can log on at a time. Each currently logged on host computer user can start *VNC Server* in Virtual Mode, and all instances, for all users, run concurrently. Note that all instances, in either mode, must listen on different ports; see *Configuring network communications* on page 86 for more information.

VNC Server can run as many times as the host computer's license permits. Each time a host computer user starts *VNC Server* (whether in User Mode or in Virtual Mode), the count of the remaining permitted desktops (that is, instances of *VNC Server*) is decremented. To see how many desktops are left, type `vnclicense -check` at the command line. For example, the message:

```
3/5 desktops.  
  johndoe : 2 desktops.  
  janedoe : 1 desktops.
```

means that five *VNC Server* desktops are licensed to run concurrently on this host computer, and three are already running: two started by John Doe, and one by Jane Doe. Two are left to run.

Note: You can release licenses by killing desktops. To see how to do this, read *Stopping VNC Server* on page 92.

Mac OS X

Under Mac OS X, a user with administrative privileges can start *VNC Server* in Service Mode. This means *VNC Server* runs, and users can connect, irrespective of whether or not a host computer user is currently logged on. (Note that connections are terminated on log off, but a disconnected user can reconnect after a few seconds.) By default, connecting users must know the user name and password of a member of the admin group in order to connect. Once connected, they have the same privileges (that is, access rights) as the *currently logged on host computer user*. For more information on privileges, see *Authenticating connections to VNC Server* on page 94.

Depending on the terms of the license, a host computer user can also, or alternatively, log on and start *VNC Server* in User Mode. This means *VNC Server* runs, and users can connect, just while this host computer user is logged on. (Connections are terminated on log off, though not on switch out if Fast User Switching is enabled.) By default, connecting users must know the user name and password of the host computer user starting *VNC Server* in order to connect. Once connected, they have the same privileges (that is, access rights) as this host computer user. For more information on privileges, see *Authenticating connections to VNC Server* on page 94.


Under Mac OS X, providing Fast User Switching is turned on, more than one host computer user can log on at a time. Each currently logged on host computer user can start *VNC Server* in User Mode, and all instances, for all users, run concurrently. Note that all instances, in either mode, must listen on different ports; see *Configuring network communications* on page 86 for more information.

VNC Server can run as many times as the host computer's license permits. Each time a host computer user starts *VNC Server* (whether in Service Mode or in User Mode), the count of the remaining permitted desktops (that is, instances of *VNC Server*) is decremented. To see how many desktops are left, type `/library/vnc/vnclicense -check` in a Terminal window. For more information on the message that is displayed, see the UNIX and Linux section above.

Working with VNC Server

This section explains basic *VNC Server* features and operations.

Using the VNC Server icon

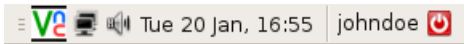
While *VNC Server* is running, a *VNC Server* icon  is displayed:

- Under Windows, in the Notification area:



(Windows XP)

- Under most versions of UNIX or Linux, for *VNC Server* in User Mode, in the Notification Area:



(Ubuntu 8.10 Linux)

Note: A *VNC Server* icon cannot be displayed for *VNC Server* in User Mode under some versions of UNIX, and for *VNC Server* in Virtual Mode under all versions of UNIX or Linux. To see how to work with *VNC Server* in Virtual Mode, read *Working with VNC Server in Virtual Mode (UNIX or Linux only)* on page 75.

- Under Mac OS X, in the Status bar:



(Mac OS X 10.5)

The *VNC Server* icon:

- Provides visual confirmation that *VNC Server* is running on the host computer. If the icon is not visible (and not hidden by other icons), then *VNC Server* is not running.
- Provides visual confirmation that *VNC Server* is configured correctly on the host computer. If not, a red error glyph appears:



Open the **VNC Server Status** dialog to begin diagnosing the problem. For more information, see *Using the VNC Server Status dialog* on page 81.

- Confirms whether users are connected or not. When the first user connects, the icon is shaded black:



When the last user disconnects, the icon reverts color again.

- Provides convenient notification of the host computer’s network address. Hover the mouse cursor over the icon:



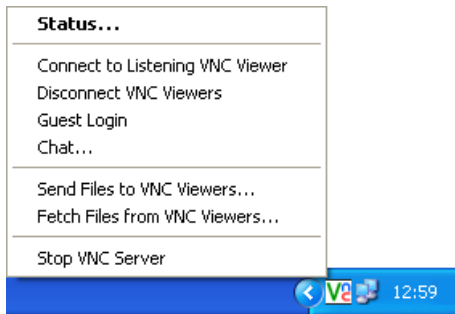
(Windows XP)

- Has a shortcut menu that performs useful operations, such as opening the **VNC Server Status** dialog. For more information, see *Using the VNC Server shortcut menu* on page 80.

Note: When a user connects, the *VNC Server* icon is displayed in the *VNC Viewer* window, as are all desktop artifacts. The connected user can open the **VNC Server Status** dialog, but cannot normally configure *VNC Server*. For more information, see *Using the VNC Server Status dialog* on page 81.

Using the VNC Server shortcut menu

VNC Server has a shortcut menu to facilitate common operations. To show it, right-click (click under Mac OS X) the *VNC Server* icon:



(Windows XP. *VNC Server* is in User Mode.)

The following table explains the effect of selecting each *VNC Server* shortcut menu option.

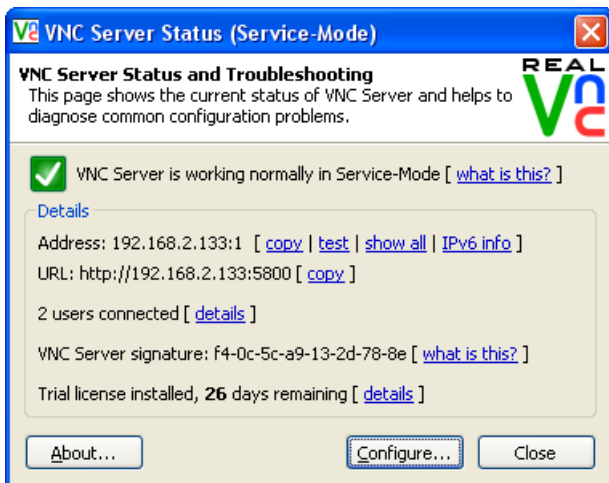
| Shortcut menu option | Explanation |
|---------------------------------|--|
| Status | Opens the VNC Server Status dialog. For more information, see <i>Using the VNC Server Status dialog</i> on page 81. |
| Connect to Listening VNC Viewer | Establishes a reverse connection to a client computer. For more information, see <i>Establishing a reverse connection</i> on page 104. |
| Disconnect VNC Viewers | Disconnects all users (including web browser users). Note that, by default, they can immediately reconnect. |
| Guest Login | When turned on, and providing <i>VNC Server</i> is configured correctly, allows a Guest to connect, bypassing <i>VNC Server</i> 's authentication mechanism. For more information, see <i>Allowing a Guest to connect</i> on page 102. |

| Shortcut menu option | Explanation |
|------------------------------|---|
| Chat | Opens a dialog where you can chat with connected <i>VNC Viewer</i> users (though not with web browser users). For more information, see <i>Communicating securely using VNC Chat</i> on page 67. |
| Send Files to VNC Viewers | Opens a dialog where you (or a connected <i>VNC Viewer</i> user) can browse to the location of host computer files to send to client computers. Note this option is disabled until a <i>VNC Viewer</i> user connects. For more information, see <i>Transferring files between client and host computers</i> on page 62. This menu option is not available for <i>VNC Server</i> in Service Mode under Windows. This feature is not available to connected web browser users. |
| Fetch Files from VNC Viewers | This option is only available if at least one client computer has made files available for the host computer to fetch. A dialog opens where you (or a connected <i>VNC Viewer</i> user) can browse to a location to put shared client computer files. For more information, see <i>Transferring files between client and host computers</i> on page 62. This menu option is not available for <i>VNC Server</i> in Service Mode under Windows. This feature is not available to connected web browser users. |
| Stop VNC Server | Stops <i>VNC Server</i> , disconnecting all users. You may be required to confirm this operation. For more information, see <i>Stopping VNC Server</i> on page 92. |

Using the VNC Server Status dialog

The **VNC Server Status** dialog is the gateway to *VNC Server*, and the first port of call for connection information and problem diagnosis. It also provides access to the **VNC Server Properties** dialog, enabling you to configure *VNC Server*.

Note: A connected user can open the **VNC Server Status** dialog but cannot configure *VNC Server* unless logged on as a host computer user with administrative privileges. For more information on privileges, see *Authenticating connections to VNC Server* on page 94.



(Windows XP)

To open the **VNC Server Status** dialog:

- Under Windows, right-click the *VNC Server* icon and, from the shortcut menu, select **Status**. (You can also just double-click the *VNC Server* icon.)
- Under UNIX or Linux, for *VNC Server* in User Mode, click the *VNC Server* icon.
- Under Mac OS X, click the *VNC Server* icon and, from the shortcut menu, select **Status**.

Note: Under UNIX or Linux, for *VNC Server* in Virtual Mode, no **VNC Server Status** dialog can be displayed. To see how to work with *VNC Server* in this mode, read *Working with VNC Server in Virtual Mode (UNIX or Linux only)* on page 75.

The title bar of the **VNC Server Status** dialog confirms which mode *VNC Server* is running in. For more information on modes, see *Running multiple instances of VNC Server* on page 76.



The **VNC Server Status** dialog provides access to the **VNC Server Properties** dialog, enabling you to configure *VNC Server*. To open it, click the **Configure** button. You may be required to confirm this operation. For more information, start with *Using the VNC Server Properties dialog* on page 85.

Diagnosing problems

The **VNC Server Status** dialog displays a green tick if *VNC Server* is configured correctly and the host computer is connected to a network:



This should mean users can immediately connect.

If an amber warning  or red error  is shown instead, click the [\[details\]](#) link that appears in the **Details** area to begin diagnosing the problem:



For more information, start with *Configuring network communications* on page 86.

Identifying the host computer

The **VNC Server Status** dialog confirms:

- The network address of the host computer, and a port number if *VNC Server* is listening for connection requests on a port other than the registered default, 5900:



In the example above, *VNC Server* is running on host computer 192.168.2.133 and listening on port 5901. Users need this information in order to connect to *VNC Server* running on a host computer within a private network (click the [\[copy\]](#) link to copy it to the Clipboard, and paste to an email or similar). If the host computer is protected by a router, users connecting over the Internet must enter the router's network address instead. To find out what this might be, click the [\[test\]](#) link. For more information on these issues, see *Step 3: Identify VNC Server on the host computer* on page 17.

The host computer may have more than one network address (for example, it may have an IPv4 and an IPv6 address). Users can enter any valid network address in order to connect to *VNC Server*. To see all the network addresses, click the [\[show all\]](#) link. Note that IPv6 addresses are unavailable for the host computer if the [\[IPv6 info\]](#) link is visible; see *Preventing connections from particular client computers* on page 106 for more information.

- The URL of the host computer and the port number on which *VNC Server* is listening for *VNC Viewer for Java* download requests:

URL: <http://192.168.2.133:5800> [\[copy\]](#)

In this example, *VNC Server* is running on host computer 192.168.2.133 and listening on port 5800. Web browser users need this information in order to download *VNC Viewer for Java* from *VNC Server*. For more information, see *Downloading VNC Viewer for Java* on page 50.

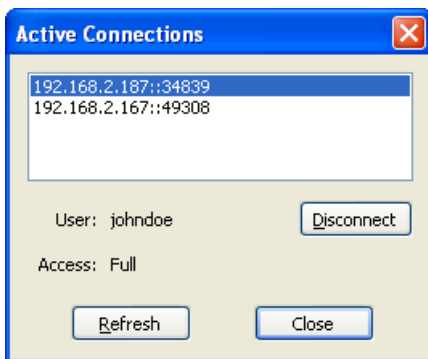
Note that *VNC Server* must listen on a unique port, and that port conflicts disable *VNC Server*. For more information, see *Configuring network communications* on page 86.

Confirming the number of connected users

The **VNC Server Status** dialog confirms the number of currently connected users:

2 users connected [\[details\]](#)

Click the [\[details\]](#) link to manage connected users. The **Active Connections** dialog opens:



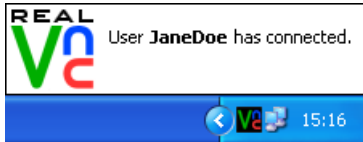
(Windows XP)

In this example, the connected user at client computer 192.168.2.187:

- Authenticated to *VNC Server* using the credentials of johndoe. This is likely to be a host computer user but, depending on *VNC Server's* authentication mechanism, this text could alternatively read `Admin` or `Guest`, or be left blank. For more information on authentication, start with *Authenticating connections to VNC Server* on page 94.
- Has a Full set of VNC permissions, permitting unrestricted access to *VNC Enterprise Edition* functionality while the connection is in progress. For more information, see *Restricting functionality for particular connected users* on page 110.

Click the **Disconnect** button to disconnect the selected user. Note there is no way of distinguishing between *VNC Viewer* and web browser users.

A host computer user is informed when a user connects by a connection prompt that appears temporarily in the bottom right hand corner of the desktop (top right under Mac OS X):



(Windows XP)

You can configure *VNC Server* so that this prompt enables the host computer user to *reject* particular connection requests. For more information, see *Preventing particular users connecting* on page 108.

Displaying the VNC Server signature

The **VNC Server Status** dialog displays a signature uniquely identifying *VNC Server*:

VNC Server signature: f4-0c-5c-a9-13-2d-78-8e [[what is this?](#)]

When a user connects to *VNC Server* for the first time, they are asked to verify this signature. For more information on this security feature, see *Uniquely identifying VNC Server* on page 114.

Warning of trial license expiry

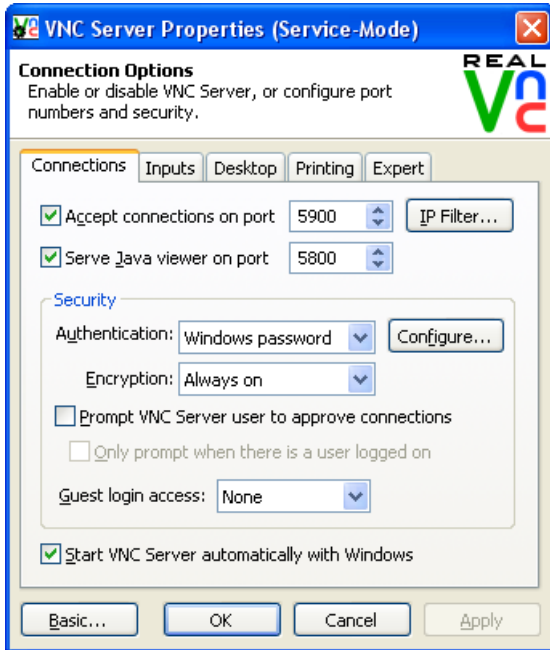
The **VNC Server Status** dialog confirms the number of days left if *VNC Enterprise Edition* was unlocked using a time-limited trial license key:

Trial license installed, 26 days remaining [[details](#)]

Click the [[details](#)] link to begin upgrading to a full, permanent license.

Using the VNC Server Properties dialog

The **VNC Server Properties** dialog enables you to configure *VNC Server*:



(Windows XP. In this example, the dialog is in Advanced mode.)

To open the **VNC Server Properties** dialog, click the **Configure** button in the **VNC Server Status** dialog. For more information on this dialog, see *Using the VNC Server Status dialog* on page 81. Under UNIX or Linux, you must further select the **Options** menu option. You may be required to confirm this operation.

Note: Under UNIX or Linux, for *VNC Server* in Virtual Mode, no **VNC Server Properties** dialog can be displayed. To see how to work with *VNC Server* in this mode, read *Working with VNC Server in Virtual Mode (UNIX or Linux only)* on page 75.

The first time you open this dialog, it opens in Basic mode, and only one tab is available, containing the most common properties. Click the **Advanced** button in the bottom left corner to switch to Advanced mode and see all the tabs in the example above. Note that the **Expert** tab is recommended for expert users only.

For information on most of the properties in this dialog, see the subsequent sections in this chapter, starting with *Configuring network communications* on page 86. For more information on the properties in the **Security** area of the **Connections** tab, and security in general, see *Chapter 7, Security* on page 93.

Note that configuring a property affects all future connections. Unless otherwise stated in the sections that follow, configuring a property affects currently connected users as well.

Configuring network communications

VNC Server listens for network communications—that is, for connection requests and for *VNC Viewer for Java* download requests—on one or more *ports*.

By default, two separate ports are assigned when *VNC Server* starts, one for connection and one for download requests. If available, then:

- Under Windows and Mac OS X, *VNC Server* in both Service Mode and User Mode is assigned port 5900 for connection requests and port 5800 for download requests.
- Under UNIX or Linux, *VNC Server* in:
 - User Mode is assigned port 5900 for connection requests and port 5800 for download requests.
 - The first instance of *VNC Server* in Virtual Mode is assigned port 5901 for connection requests and port 5801 for download requests. Subsequent instances of *VNC Server* in Virtual Mode are assigned port numbers incremented by one, where possible, for example 5902, 5903 (and 5802, 5803), and so on, up to the maximum number of desktops permitted by the host computer's license.

Note: For more information about running multiple instances of *VNC Server*, and the different modes, see *Running multiple instances of VNC Server* on page 76.

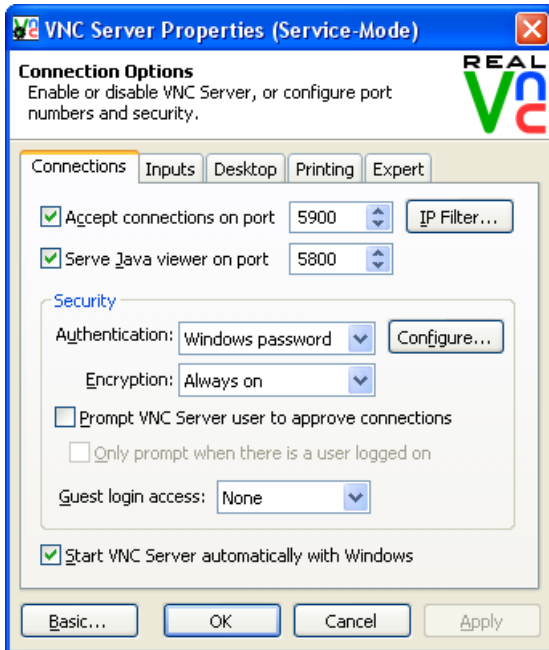
If more than one instance of *VNC Server* is running on a host computer, they must all listen on different ports; see below for information on resolving port conflicts. Note, however, that a particular instance of *VNC Server* can listen on the *same* port for connection and download requests; see *Making the connection and download port the same* on page 88 for more information.

Note: When connecting to *VNC Server*, a user must qualify the host computer's network address with the port number in all cases *except* when *VNC Server* is listening for connection requests on port 5900 only. For more information, see *Qualifying a network address with a port number* on page 24.

Resolving port conflicts

VNC Server must listen for connection and for *VNC Viewer for Java* download requests on a unique port. This is one on which no other instance of *VNC Server* running on the host computer, or any other service or program, is listening.

Port conflicts disable *VNC Server*. You should be able to resolve them by changing the ports on which *VNC Server* listens. To do this, configure properties on the **Connections** tab of the **VNC Server Properties** dialog. For more information on this dialog, see *Using the VNC Server Properties dialog* on page 85.



(Windows XP)

Changing the connection port

You can change the port on which *VNC Server* is listening for connection requests. If you do this:

- Users need to know the new port number (if it is not 5900) in order to enter it when connecting. For more information, see *Qualifying a network address with a port number* on page 24.
- If the host computer is protected by a firewall, then the firewall must be configured to allow incoming network communications to the new port. For more information, see *Allowing network communications through a firewall* on page 26.
- If the host computer is protected by a router and users will connect over the Internet, then the router must be configured to forward communications to the new port. For more information, see *Configuring a router to forward network communications* on page 23.

To change the port, enter a different number in the **Accept connections on port** field. Note that configuring this property does not affect currently connected users.

Changing the download port

You can change the port on which *VNC Server* is listening for *VNC Viewer for Java* download requests. If you do this:

- Web browser users need to know the new port number in order to enter it when downloading. For more information, see *Qualifying a network address with a port number* on page 24.
- If the host computer is protected by a firewall, then the firewall must be configured to allow incoming network communications to the new port. For more information, see *Allowing network communications through a firewall* on page 26.
- If the host computer is protected by a router and web browser users will connect over the Internet, then the router must be configured to forward communications to the new port. For more information, see *Configuring a router to forward network communications* on page 23.

To change the port, enter a different number in the **Serve Java viewer on port** field. Note that configuring this property does not affect currently connected users.

Making the connection and download port the same

VNC Server can listen on the same port for connection and download requests. This may simplify firewall configuration and make the host computer more secure.

To use the same port, enter the same number in the **Accept connections on port** and **Serve Java viewer on port** fields. Note that configuring these properties does not affect currently connected users.

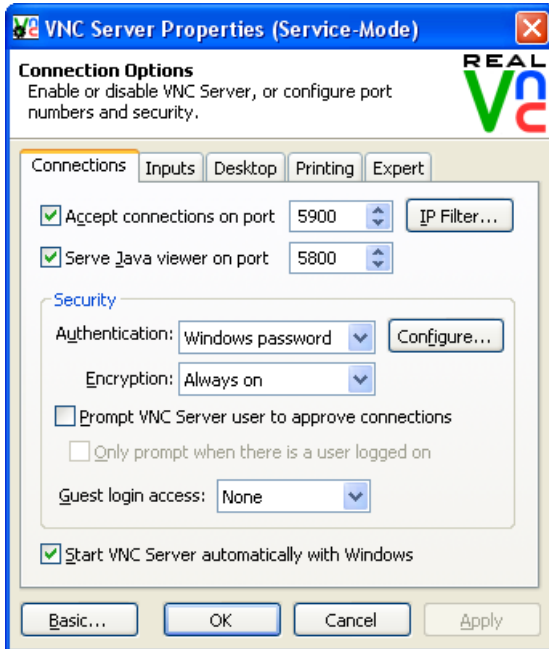
Preventing connections to VNC Server

By default, as soon as *VNC Server* starts:

- Users can connect to *VNC Server* and begin controlling the host computer.
- Web browser users can download *VNC Viewer for Java*, and use it to connect to this or to another host computer.

You can prevent all users connecting by configuring properties on the **Connections** tab of the **VNC Server Properties** dialog. For more information on this dialog, see *Using the VNC Server Properties dialog* on page 85.

Note: You can prevent *particular* users connecting, or connections from *particular* client computers. For more information, see *Preventing particular connections to VNC Server* on page 106.



(Windows XP)

Preventing all connections

You can prevent all users connecting to *VNC Server*. To do this, turn off **Accept connections on port**. Note that configuring this property does not affect currently connected users.

Note: If the **VNC Server Properties** dialog is in Basic mode, this option is called **Allow VNC Viewers to connect to VNC Server**.

You can still use *VNC Server* to establish a reverse connection to a client computer. For more information, see *Establishing a reverse connection* on page 104.

Preventing all VNC Viewer for Java downloads

You can prevent all web browser users downloading *VNC Viewer for Java* from *VNC Server*. To do this, turn off **Serve Java viewer on port**. Note that configuring this property does not affect currently connected users.

Restricting functionality for connected users

By default, any number of users can connect to an instance of *VNC Server* running on a host computer. Each connected user can:

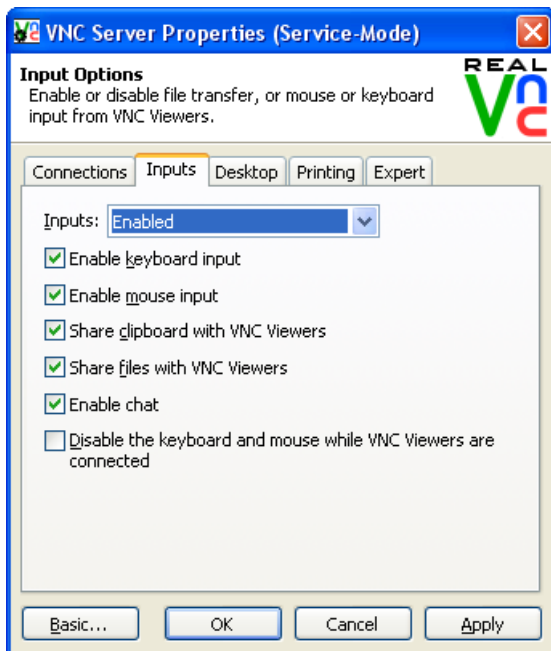
- Control the host computer using the client computer's keyboard and mouse, for example by running applications, changing settings, and accessing data (according to their privileges on the host computer).
- Copy and paste text between applications running on the client and host computers.

In addition, each connected *VNC Viewer* user can:

- Print host computer files to a printer attached to the client computer.
- Exchange files with the host computer.
- Chat with other *VNC Viewer* users connected to the same host computer, or with a host computer user.

You can restrict access to *VNC Enterprise Edition* functionality for all connected users, if necessary, by configuring properties on the **Inputs** tab of the **VNC Server Properties** dialog. For more information on this dialog, see *Using the VNC Server Properties dialog* on page 85.

Note: You can restrict access to *VNC Enterprise Edition* functionality for *particular* users by revoking VNC permissions. For more information, see *Restricting functionality for particular connected users* on page 110.



(Windows XP)

Making VNC Server ‘view only’

You can quickly prevent all interchange with all client computers, making *VNC Server* ‘view only’. This might be useful in an educational environment, for example, when multiple users are connected but should not interact. To do this, select `Disabled (view-only mode)` from the **Inputs** dropdown.

Disabling the keyboards of client computers

You can disable the keyboards of all client computers. To do this, turn off **Enable keyboard input**.

Disabling the mice of client computers

You can disable the mice of all client computers. To do this, turn off **Enable mouse input**.

Preventing printing

You can prevent all *VNC Viewer* users printing host computer files to local printers. To do this, turn off **Allow VNC Viewers to share printers**. Note this property is on the **Printing** tab. For more information about this feature, see *Printing host computer files to a local printer* on page 60.

Under UNIX or Linux, if you have root privileges on the host computer, you can disable printing system-wide. To do this, type `vncinitconfig -disable-print` in a Terminal window, and press the ENTER key. The **Printing** tab is disabled. To reverse this, type `vncinitconfig -enable-print`.

Under Windows, if you have sufficient privileges on the host computer, you can disable printing system-wide by re-installing *VNC Enterprise Edition* without the VNC Printer Driver component. To do this, turn off **VNC Printer Driver** at the appropriate step in the Installation Wizard. For more information on how to do this, see the RealVNC web site. The **Printing** tab is disabled.

Preventing file transfer

You can prevent all *VNC Viewer* users exchanging files with the host computer. To do this, turn off **Share files with VNC Viewers**. For more information about this feature, see *Transferring files between client and host computers* on page 62.

Preventing copy and paste

You can prevent all users copying and pasting text between applications running on the client and host computers. To do this, turn off **Share clipboard with VNC Viewers**. For more information about this feature, see *Copying and pasting text between client and host computers* on page 66

Note: Under Windows, to prevent connected *VNC Viewer* users who are also running Windows from copying and pasting *files*, turn off **Share files with VNC Viewers**.

Preventing chat

You can prevent *VNC Viewer* users communicating securely using *VNC Chat*. To do this, turn off **Enable chat**. For more information about this feature, see *Communicating securely using VNC Chat* on page 67.

Stopping VNC Server

VNC Server runs until it is stopped.

To explicitly stop VNC Server:

- Under Windows, right-click the VNC Server icon in the Notification area and, from the shortcut menu, select **Stop VNC Server**.
- Under UNIX or Linux, to stop VNC Server:
 - In User Mode, right-click the VNC Server icon in the Notification Area and, from the shortcut menu, select **Stop VNC Server**.
 - In Virtual Mode, type `vncserver -kill :x` at the command line, where `x` is the X Server session number. For more information on this, see page 73.
- Under Mac OS X, click the VNC Server icon in the Status bar and, from the shortcut menu, select **Stop VNC Server**.

You may be required to confirm this operation.

Note: For more information on the VNC Server icon and shortcut menu, see *Working with VNC Server* on page 79.

Note that VNC Server automatically stops:

- In User Mode (all platforms), when the host computer starting it logs out or the host computer is powered off.
- In Service Mode (Windows and Mac OS X), when the host computer is powered off. Under Windows, by default, VNC Server starts again automatically when the computer is powered on. To see how to prevent this, read *Preventing VNC Server starting automatically (Windows only)* on page 75.
- In Virtual Mode (UNIX or Linux), when the host computer is powered off.

VNC Server can also stop under the following circumstances:

- Under Windows, VNC Server in User Mode stops automatically when the last user disconnects if the **When last VNC Viewer disconnects** property is changed to `Logoff user`. For more information, see *Protecting the host computer* on page 115.
- A connected user logged on as a host computer user with administrative privileges can explicitly stop VNC Server.
- A connected user can log out and power the host computer off.

To see how to start VNC Server again, read *Starting VNC Server* on page 72.

7

Security

VNC Enterprise Edition is designed to establish authenticated, encrypted connections between a host and one or more client computers. This chapter explains how to relax the authentication and encryption rules if you are sure all potential client computers are within a secure network environment, and all potential users are trustworthy.

This chapter also explains how to configure *VNC Server* to protect the host computer from accidental or malicious damage by *particular* users, either by restricting their access to *VNC Enterprise Edition* functionality while connections are in progress, or by preventing them connecting in the first place.

Contents

| | |
|--|-----|
| Authenticating connections to VNC Server | 94 |
| Relaxing the authentication rules | 99 |
| Bypassing the authentication rules | 102 |
| Relaxing the encryption rules | 105 |
| Preventing particular connections to VNC Server | 106 |
| Restricting functionality for particular connected users | 110 |
| Uniquely identifying VNC Server | 114 |
| Upholding privacy | 115 |

Authenticating connections to VNC Server

By default, a user must authenticate in order to connect to *VNC Server*. Note this is not the same as logging on to the host computer.

VNC Enterprise Edition is designed to be secure so authentication rules are strict out-of-the-box. You can relax the rules, or bypass them altogether, if you consider it safe to do so. For more information, start with *Relaxing the authentication rules* on page 99.

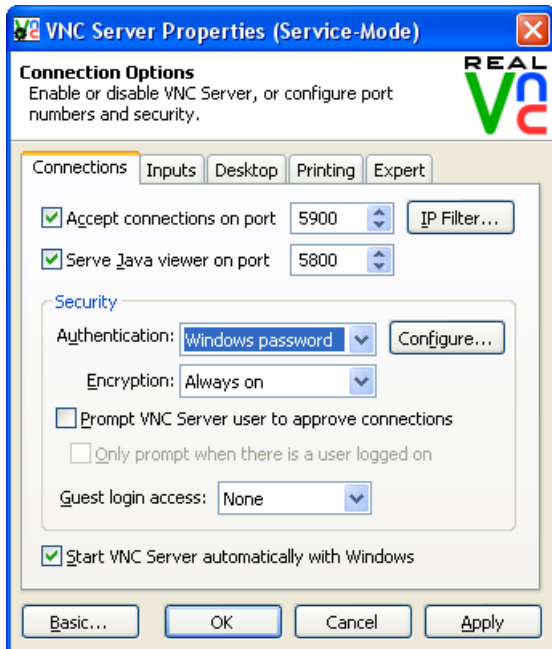
By default, under all platforms, *VNC Server* specifies *platform-native authentication*. This means that a user must supply the credentials (that is, a user name and password) of a *host computer user* in order to connect. For more information, read the section appropriate to the platform of the host computer below.

Note: Platform-native authentication is not available in *VNC Personal Edition*. The default authentication mechanism is `VNC password`.

Note that in some circumstances, a host computer user might not have set a password on the primary user account (this may be the case when connecting to friends and family, for example). In this circumstance, the default authentication mechanism must be changed to `VNC password`, or else authentication disabled. A user cannot specify a blank password in order to connect.

Windows

Under Windows, platform-native authentication is specified by the default `Windows password` option in the **Authentication** dropdown of the **VNC Server Properties** dialog. For more information on this dialog, see *Using the VNC Server Properties dialog* on page 85.



(Windows XP)

This means, to connect to *VNC Server*:

- In Service Mode, a user must supply the credentials of a member of the Administrators group.
- In User Mode, a user must supply either:
 - The credentials of the currently logged on host computer user (that is, the user starting *VNC Server*).
 - The credentials of a member of the Administrators group.

You can add different users or groups to the authentication list if you do not want to distribute the credentials of members of the Administrators group. For more information, see *Managing users and groups in the authentication list* on page 98.

Note that the credentials supplied by a user in order to connect to *VNC Server* determine the VNC permissions granted to that user. VNC permissions control which features of *VNC Enterprise Edition* a connected user is allowed to use. By default:

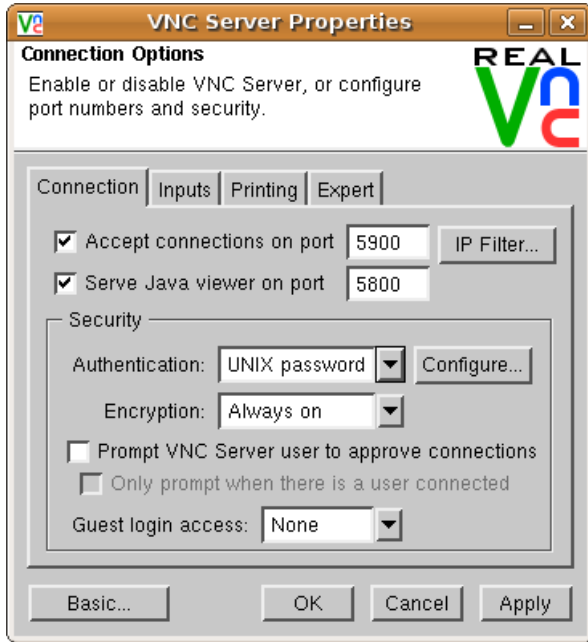
- If the credentials of a member of the Administrators group were supplied, a Full set of VNC permissions is granted to the connected user.
- If the credentials of any other host computer user were supplied, a Default set of VNC permissions is granted.

For more information on what this means, and how to revoke VNC permissions in order to restrict access to functionality, see *Restricting functionality for particular connected users* on page 110.

Once connected, a user has the same privileges (that is, access rights) on the host computer as the *currently logged on host computer user*. This need not be a user with administrative privileges even if the credentials of one were supplied in order to connect to *VNC Server*. The opposite also holds true: a connected user has administrative privileges on the host computer if such a user is currently logged on. Note that if *VNC Server* is running in Service Mode and no host computer user is logged on, then the connected user must log on to Windows in order to continue.

UNIX or Linux

Under UNIX or Linux, platform-native authentication is specified by the default UNIX password option in the **Authentication** dropdown of the **VNC Server Properties** dialog. For more information on this dialog, see *Using the VNC Server Properties dialog* on page 85.



(Ubuntu 8.10 Linux)

This means, to connect to *VNC Server* in either User Mode or in Virtual Mode, a user must supply the credentials of the host computer user starting *VNC Server*. You can add different users or groups to the authentication list if you do not want to distribute the credentials of this host computer user. For more information, see *Managing users and groups in the authentication list* on page 98.

Note that the credentials supplied by a user in order to connect to *VNC Server* determine the VNC permissions granted to that user. VNC permissions control which features of *VNC Enterprise Edition* a connected user is allowed to use. By default, a Full set of VNC permissions is granted. For more information on what this means, and how to revoke VNC permissions in order to restrict access to functionality, see *Restricting functionality for particular connected users* on page 110.

Once connected, a user has the same privileges (that is, access rights) on the host computer as the host computer user starting *VNC Server*. This need not be a user with administrative privileges even if the credentials of one were supplied in order to connect to *VNC Server*. The opposite also holds true: a connected user has administrative privileges on the host computer if such a user started *VNC Server*.

Mac OS X

Under Mac OS X, platform-native authentication is specified by the default `Mac password` option in the **Authentication** dropdown of the **VNC Server Properties** dialog. For more information on this dialog, see *Using the VNC Server Properties dialog* on page 85.



(Mac OS X 10.5)

This means, to connect to VNC Server:

- In Service Mode, a user must supply the credentials of a member of the admin group.
- In User Mode, a user must supply the credentials of the host computer user starting VNC Server.

You can add different users or groups to the authentication list if you do not want to distribute the credentials of host computer users with administrative privileges. For more information, see *Managing users and groups in the authentication list* on page 98.

Note that the credentials supplied by a user in order to connect to VNC Server determine the VNC permissions granted to that user. VNC permissions control which features of VNC Enterprise Edition a connected user is allowed to use. By default, a Full set of VNC permissions is granted. For more information on what this means, and how to revoke VNC permissions in order to restrict access to functionality, see *Restricting functionality for particular connected users* on page 110.

Once connected to VNC Server:

- In Service Mode, a user has the same privileges (that is, access rights) as the currently logged on host computer user. If no host computer user is logged on, then the user must log on in order to continue.
- In User Mode, a user has the same privileges as the host computer user starting VNC Server.

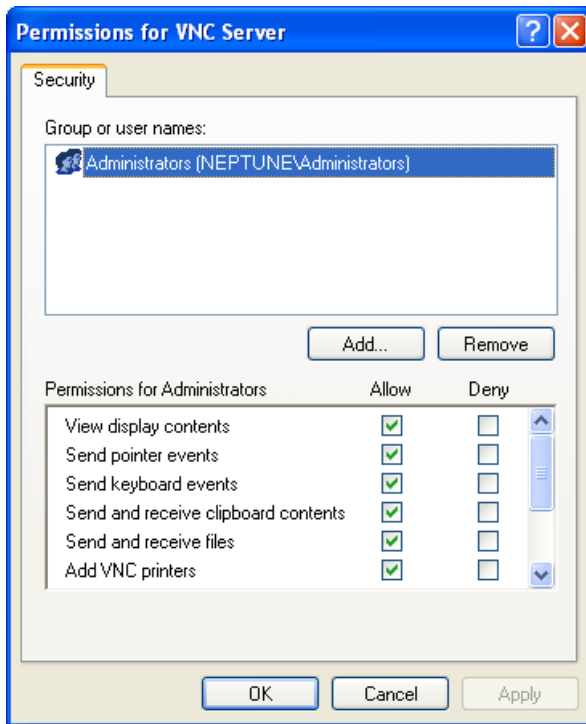
In either case, this need not be a host computer user with administrative privileges even if the credentials of one were supplied in order to connect to VNC Server. The opposite also holds true: a connected user has administrative privileges on the host computer if such a user either started VNC Server (User Mode) or is currently logged on (Service Mode).

Managing users and groups in the authentication list

By default, *VNC Server* specifies platform-native authentication, which means that a user must supply the credentials of a host computer user in order to connect to *VNC Server*. Under certain circumstances, this may be the credentials of a host computer user with administrative privileges.

If you want to use platform-native authentication but do not want to distribute the credentials of host computer users with administrative privileges, you can add host computer users or groups with less sensitive credentials to the *VNC Server* authentication list. (Alternatively, you could just choose a different authentication mechanism; for more information, see *Relaxing the authentication rules* on page 99.)

To manage users and groups in the authentication list, open the **VNC Server Properties** dialog. For more information on this dialog, see *Using the VNC Server Properties dialog* on page 85. On the **Connections** tab, click the **Configure** button. Providing either `Windows password` (or equivalent) or `Single sign-on` is selected in the **Authentication** dropdown, then the **Permissions for VNC Server** dialog opens:



(Windows XP)

To add a new host computer user or group, click the **Add** button. To remove an existing host computer user or group, select it in the list and click the **Remove** button. Note that a user can supply the credentials of *any* of the host computer users listed in **Group or user names** in order to connect to *VNC Server*.

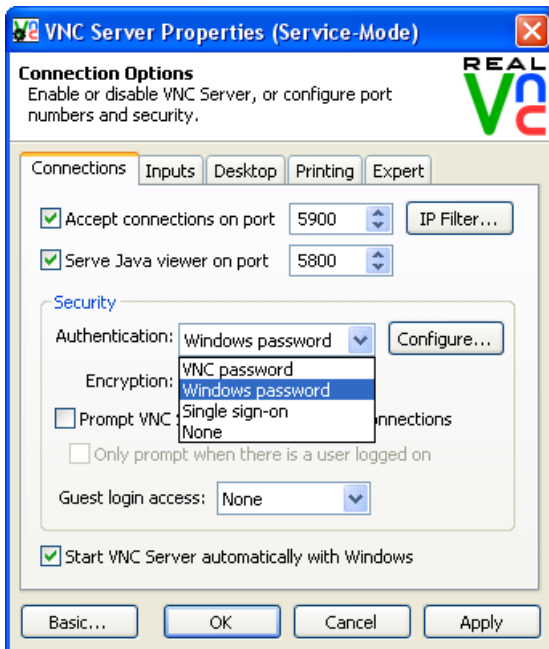
Note that when you add a new host computer user or group to the authentication list, a Default set of VNC permissions is granted to users supplying those credentials in order to connect, even if this host computer user or group has administrative privileges on the host computer. For more information on VNC permissions, see *Restricting functionality for particular connected users* on page 110.

Relaxing the authentication rules

By default, *VNC Server* specifies platform-native authentication, which means that a user must supply the credentials of a host computer user in order to connect to *VNC Server*. For more information, see *Authenticating connections to VNC Server* on page 94.

You can relax the authentication rules by choosing an alternative authentication mechanism. Depending on your choice, this may speed up the connection process, prevent ‘password fatigue’, or forgo the need to distribute host computer user credentials. Note that some mechanisms allocate VNC permissions in ways that cannot be customized.

To change the authentication mechanism, open the **VNC Server Properties** dialog. For more information on this dialog, see *Using the VNC Server Properties dialog* on page 85. On the **Connections** tab, select an alternative to the default `Windows password` option from the **Authentication** dropdown:



(Windows XP)

Note: Under UNIX or Linux, `Windows password` is called `UNIX password`. Under Mac OS X, it is called `Mac password`.

For more information on the alternative authentication mechanisms, read the appropriate section below.

Single sign on

The `Single sign-on` authentication mechanism extends platform-native authentication to automatically authenticate a *VNC Viewer* user to any instance of *VNC Server* on any host computer using the credentials used to log on to the client computer. For this to work, all host computers must be on a domain, and all instances of *VNC Server* must have `Single sign-on` specified. Note that this feature is not available for

VNC Viewer for Java; web browser users must always supply a user name and password in order to connect.

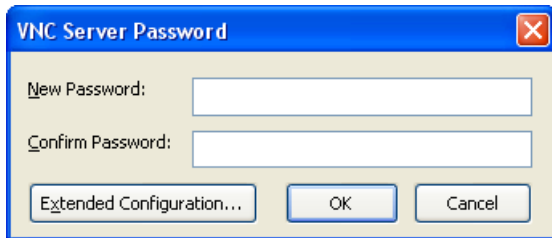
VNC permissions are granted in the same way as for platform-native authentication, and can be customized. For more information, see the appropriate platform-specific section in *Authenticating connections to VNC Server* on page 94.

VNC password

The VNC password authentication mechanism disassociates *VNC Server* from the credentialing system of the host computer. Instead, a user must supply a password of your choice in order to connect to *VNC Server*. You can specify three types of password, each of which grants a different set of VNC permissions to connected users.

Note: VNC password is the default authentication mechanism in *VNC Personal Edition*.

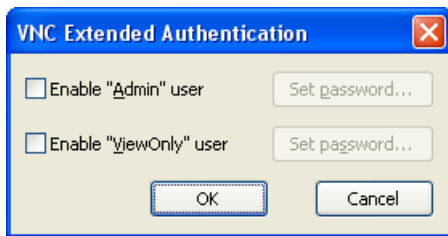
To do this, select VNC password from the **Authentication** dropdown, and click the **Configure** button. The **VNC Server Password** dialog opens:



(Windows XP)

To grant connected users a Default set of VNC permissions, enter and confirm a generic password, and click the **OK** button.

To grant connected users either a Full or a View Only set of VNC permissions, click the **Extended Configuration** button. The **VNC Extended Authentication** dialog opens:

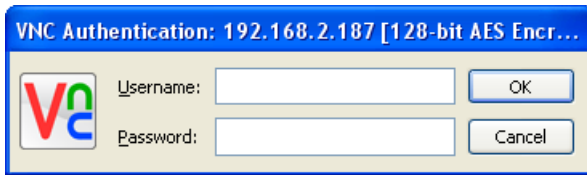


(Windows XP)

To grant to connected users:

- A Full set of VNC permissions, turn on **Enable “Admin” user**, and click the adjacent **Set password** button to enter and confirm a password.
- A View Only set of VNC permissions, turn on **Enable “ViewOnly” user** and click the adjacent **Set password** button to enter and confirm a password.

When connecting to VNC Server, a user is presented with the **VNC Authentication** dialog:



(Windows XP)

If the user enters:

- The generic password in the **Password** field, leaving the **Username** field empty (if it is enabled at all), a Default set of VNC permissions is granted.
- Admin in the **Username** field, and the appropriate password in the **Password** field, a Full set of VNC permissions is granted.
- ViewOnly in the **Username** field, and the appropriate password in the **Password** field, a View Only set of VNC permissions is granted.

For more information on VNC permissions, see *Restricting functionality for particular connected users* on page 110. Note you cannot customize VNC permissions under this authentication mechanism.

None

The **None** authentication mechanism enables a user to connect to VNC Server without supplying a password. You should only choose this option if you are sure all potential users are trustworthy. Note you can allow just *particular* users to connect without supplying a password; see *Bypassing the authentication rules* on page 102 for more information.

Note: The **None** option is only available in the **Authentication** dropdown when the **VNC Server Properties** dialog is in Advanced mode. For more information, see *Using the VNC Server Properties dialog* on page 85.

A Default set of VNC permissions is granted to each connected user. For more information, see *Restricting functionality for particular connected users* on page 110. Note you cannot customize VNC permissions under this authentication mechanism.

Bypassing the authentication rules

You can enable particular users to connect to *VNC Server* without specifying a password, bypassing *VNC Server's* authentication mechanism altogether. You can:

- Allow a user to connect as a Guest. See below for more information.
- Establish a reverse connection to a client computer. See *Establishing a reverse connection* on page 104 for more information.

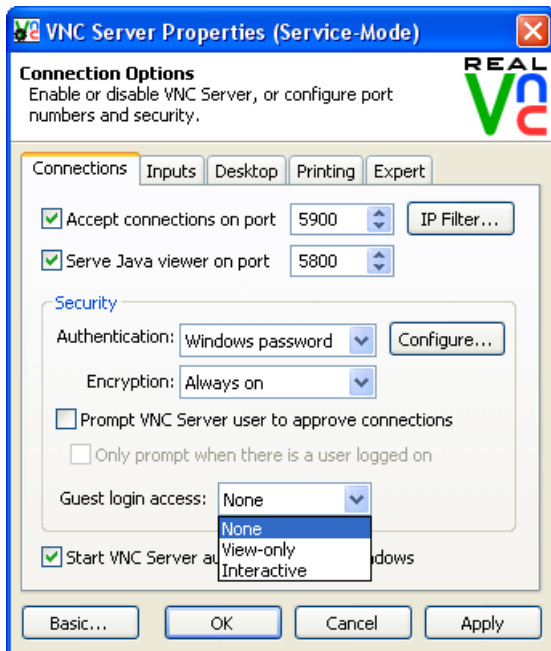
Clearly, you should only allow trustworthy users to connect as Guests, and only establish reverse connections to client computers with trustworthy potential users. If you are setting up *VNC Server* on your own computer for remote access, note that a user must be present at the host computer for both these features to work.

Note: You can enable *all* users to connect without supplying a password if you consider it safe to do so. For more information, see *Relaxing the authentication rules* on page 99.

Allowing a Guest to connect

You can allow a particular user to connect as a Guest, bypassing the authentication mechanism specified by *VNC Server*. A Guest typically connects infrequently, or for a short period of time.

To connect a Guest, open the **VNC Server Properties** dialog. For more information on this dialog, see *Using the VNC Server Properties dialog* on page 85. On the **Connections** tab, select an alternative to the default `None` option from the **Guest login access** dropdown:



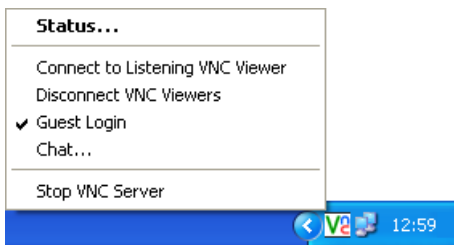
(Windows XP)

To grant to a connected Guest:

- A Default set of VNC permissions, select *Interactive*.
- A View Only set of VNC permissions, select *View-only*.

For more information on VNC permissions, see *Restricting functionality for particular connected users* on page 110. Note you cannot customize VNC permissions for Guests.

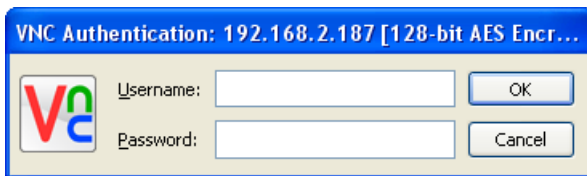
To enable a Guest to connect, a host computer user must turn on the **Guest Login** option on the **VNC Server** shortcut menu. For more information on this menu, see *Using the VNC Server shortcut menu* on page 80. For example:



(Windows XP)

Note: If the **Guest Login** menu option is turned off, Guests cannot connect. Note that connected users can turn this menu option on and off. When **VNC Server** starts, **Guest Login** is turned off by default.

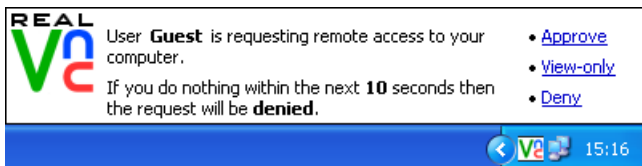
When connecting to **VNC Server**, a Guest is presented with the **VNC Authentication** dialog:



(Windows XP)

To connect, the Guest must enter *Guest* in the **Username** field, and leave the **Password** field empty.

When the connection request is received by **VNC Server**, a connection prompt appears on the host computer:



(Windows XP)

A host computer user must approve the connection request within ten seconds or it will be automatically rejected. For more information on connection prompts, see *Preventing particular users connecting* on page 108.

Establishing a reverse connection

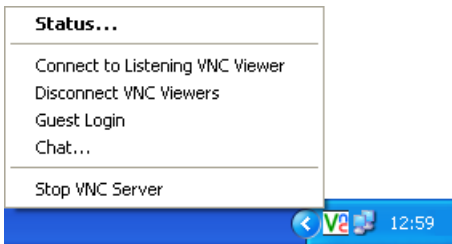
You may be able to establish a reverse connection to a particular client computer, bypassing the authentication mechanism specified by *VNC Server*.

Note: The client computer must be running *Listening VNC Viewer*. For more information, see *Starting Listening VNC Viewer* on page 30.

This feature might also be useful if the host computer is protected by a firewall that cannot be configured to allow incoming network communications, or by a router that cannot be configured to forward incoming network communications to the host computer, preventing normal connections. In a reverse connection, network communications from a host computer are *outgoing*.

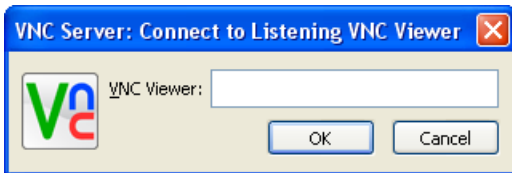
To establish a reverse connection:

1. Open the *VNC Server* shortcut menu. For more on this menu, see *Using the VNC Server shortcut menu* on page 80:



(Windows XP)

2. Select **Connect to Listening VNC Viewer**. The **Connect to Listening VNC Viewer** dialog opens:



(Windows XP)

3. Enter the network address of the client computer (or a router) in the **VNC Viewer** field, for example 192.168.2.187, and click the **OK** button.

If you do not know a network address for the client computer, and it is also running *VNC Server*, you can ask a client computer user to follow the instructions in *Step 2: Start VNC Viewer on the client computer* on page 17. If not, you will need to ask the client computer user to use a command such as `ipconfig` (Windows) or `ifconfig` (Linux and Mac OS X).

Listening VNC Viewer listens for reverse connections on port 5500. If a reverse connection fails, it may be because the client computer is protected by a router and/or a firewall and these devices have not been configured to allow access to *Listening VNC Viewer* at port 5500. For more information on this, and connection issues in general, see *Troubleshooting connection* on page 21.

When a reverse connection is established, the desktop of the host computer is displayed on the client computer in exactly the same way as it is for *VNC Viewer*. A *Listening VNC Viewer* user controls the host

computer in the same way a *VNC Viewer* user does. For more information, see *Chapter 3, Using VNC Viewer* on page 29.

A Full set of VNC permissions is granted to a *Listening VNC Viewer* user. For more information, see *Restricting functionality for particular connected users* on page 110. Note you cannot customize VNC permissions for *Listening VNC Viewer* users.

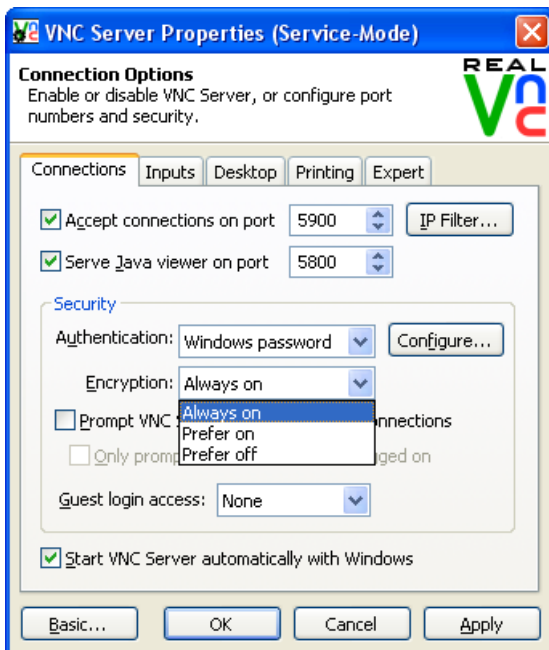
Relaxing the encryption rules

By default, all network communications between a client and host computer are encrypted using 128 bit AES technology. Authentication credentials are protected by 2048 bit RSA public keys.

You can relax the encryption rules if you are sure all potential client computers are within a secure network environment, and that eavesdropping is impossible. This may improve performance. It may also allow older versions of *VNC Viewer* that do not support encryption to connect. For more information on eavesdropping, see *Uniquely identifying VNC Server* on page 114.

Note: Even if encryption is turned off, passwords are still encrypted.

To relax the encryption rules, open the **VNC Server Properties** dialog. For more information on this dialog, see *Using the VNC Server Properties dialog* on page 85. On the **Connections** tab, select an alternative to the default `Always on` option from the **Encryption** dropdown:



(Windows XP)

For more information on the alternative encryption options, read the appropriate section below.

Prefer on

Encryption is turned on. However, a client computer user can turn it off by selecting `Prefer off` in the **VNC Viewer: New Connection** dialog before connecting to *VNC Server*.

Prefer off

Encryption is turned off. However, a client computer user can turn it back on by selecting either `Prefer on` or `Always on` in the **VNC Viewer: New Connection** dialog before connecting to *VNC Server*.

For more information about selecting encryption options when connecting to *VNC Server*, see *Step 4: Select an encryption option* on page 19.

Preventing particular connections to VNC Server

You can prevent particular users connecting to *VNC Server*. To do this, you can either:

- Prevent connections from particular client computers. See below for more information.
- Prevent particular users connecting. See *Preventing particular users connecting* on page 108 for more information.

Note: You can prevent *all* users connecting to *VNC Server*. For more information, see *Preventing connections to VNC Server* on page 88.

Preventing connections from particular client computers

You can prevent all connections originating from one or more particular client computers by filtering the network addresses of those client computers.

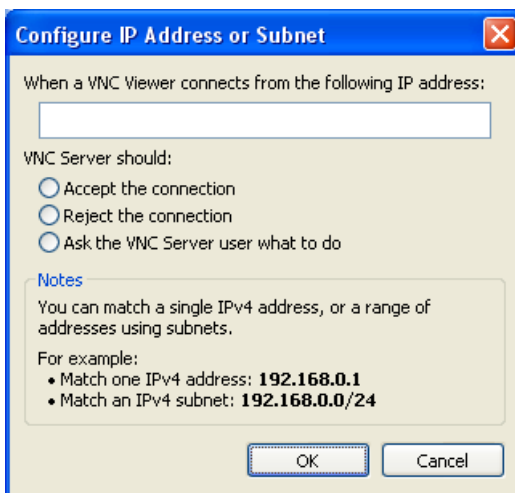
Note: If you filter network addresses, IPv6 network addresses for the *host* computer become unavailable. A user cannot enter an IPv6 network address in order to connect to *VNC Server* (even from an authorized client computer).

To filter network addresses, open the **VNC Server Properties** dialog. For more information on this dialog, see *Using the VNC Server Properties dialog* on page 85. On the **Connections** tab, click the **IP Filter** button. The **Configure IP Address Filtering** dialog opens:



(Windows XP)

By default, connection requests are accepted from all client computers. To reject connection requests from a particular client computer, click the **Add** button. The **Configure IP Address or Subnet** dialog opens:



(Windows XP)

Enter the network address, or a range of addresses, in IPv4 format, and choose one of the following options:

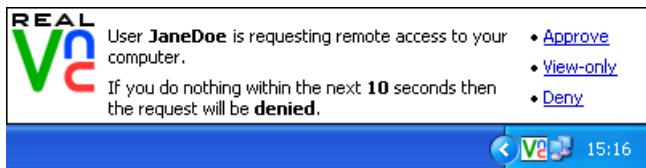
| Option | Explanation |
|------------------------------------|---|
| Accept the connection | Accepts connection requests from the client computer(s). |
| Reject the connection | Rejects connection requests from the client computer(s). |
| Ask the VNC Server user what to do | Prompts a host computer user to either accept connection requests from the client computer(s), allow them 'view only' access, or reject requests. If no host computer user is present, connection requests are automatically rejected after 10 seconds. For more information on connection prompts, see <i>Preventing particular users connecting</i> on page 108. |

Note that if you filter network addresses, the order of rules in the **Configure IP Address Filtering** dialog is important. The first matching rule determines what happens to connection requests from a particular client computer. For example, if a rule rejecting a client computer is encountered before one accepting it, then all connection requests from that client computer will always be rejected. You can move rules in the dialog using the **Up** and **Down** arrows.

By default, the `Default` rule *accepts* connection requests from all client computers. You can change this so that it rejects or queries all connection requests instead. To do this, select the `Default` rule, and click the **Edit** button. You cannot move this rule in the dialog.

Preventing particular users connecting

You can prevent a particular user connecting by causing a connection prompt to appear on the host computer's desktop:



(Windows XP)

A connection prompt enables a host computer user, if one is present, to either accept the connection request, allow 'view only' access to the host computer, or reject the request. If no host computer user is present, or if no response is received within ten seconds, then the connection request is automatically rejected. Note if you are setting up *VNC Server* on your own computer for remote access then enabling this feature may prevent you connecting.

Note that a user supplying credentials granting a Full set of VNC permissions is able to bypass connection prompts. A host computer user cannot prevent these users connecting by default. You can configure the `Connect without accept/reject prompt` permission to either permit other users to bypass connection prompts, or to submit all users, including users with Full VNC permissions, to them. For more information, see *Customizing VNC permissions* on page 111.

To cause connection prompts to appear, open the **VNC Server Properties** dialog. For more information on this dialog, see *Using the VNC Server Properties dialog* on page 85. On the **Connections** tab, turn on **Prompt VNC Server user to approve connections**:



(Windows XP)

Clearly, this feature is only useful if a host computer user is present.

Note: Under UNIX or Linux, for *VNC Server* in Virtual Mode, no host computer user is 'present'. This feature is therefore only useful if at least one user is able to bypass connection prompts. Such a user can then accept or reject subsequent connection requests.

For *VNC Server* in Service Mode, if a host computer user is only likely to be intermittently present, you should also turn on **Only prompt when there is a user logged on**. This means connection prompts will only appear if a host computer user is logged on (and therefore likely to be present). If no host computer user is logged on, connection prompts will not appear. In these circumstances, all users are able to connect, though note they must then log on to the host computer in order to continue.

Restricting functionality for particular connected users

When a user connects to *VNC Server*, a set of VNC permissions is granted to that user. VNC permissions control which features of *VNC Enterprise Edition* a connected user is allowed to use.

Note: Connected web browser users are further restricted by the limited functionality of *VNC Viewer for Java*. A web browser user cannot print even if the `Add VNC printer` permission is granted, for example. For more information on these limitations, see *Connecting from a web browser* on page 13.

The following table explains how VNC permissions are granted to users who authenticate in order to connect to *VNC Server*:

| VNC Server authentication mechanism | Credentials supplied in order to connect | Set of VNC permissions granted | Customizable? |
|--|---|--------------------------------|---------------|
| Platform-native authentication or Single sign-on | Host computer user with administrative privileges | Full | YES |
| | Any other host computer user | Default | YES |
| VNC password | Generic password (no user name) | Default | NO |
| | Admin user name and appropriate password | Full | NO |
| | ViewOnly user name and appropriate password | View Only | NO |
| None | | Default | NO |

For information on platform-native authentication, see *Authenticating connections to VNC Server* on page 94. For information on the other authentication mechanisms, see *Relaxing the authentication rules* on page 99.

The following table explains how VNC permissions are granted to users who bypass *VNC Server's* authentication mechanism:

| Type of user | Credentials supplied in order to connect | Set of VNC permissions granted | Customizable? |
|-----------------------------|--|--------------------------------|---------------|
| Guest (Interactive) | Guest user name (no password) | Default | NO |
| Guest (View-only) | | View Only | NO |
| Listening <i>VNC Viewer</i> | | Full | NO |

For more information on these types of user, see *Bypassing the authentication rules* on page 102.

The following table explains the individual permissions allocated to the three sets (Full, Default, and View Only):

| Permission name | When granted, a connected user can... | Full | Default | View Only |
|--------------------------------------|--|------|---------|-----------|
| View display contents | See the host computer's desktop. | YES | YES | YES |
| Send pointer events | Control the host computer using the client computer's mouse. | YES | YES | |
| Send keyboard events | Control the host computer using the client computer's keyboard. | YES | YES | |
| Send and receive clipboard contents | Copy and paste text between applications running on the client and host computers. | YES | YES | |
| Send and receive files | Exchange files with the host computer. <i>VNC Viewer</i> users only. | YES | YES | |
| Add VNC printers | Print host computer files to a local printer. <i>VNC Viewer</i> users only. | YES | YES | |
| Accept chat messages | Chat with other <i>VNC Viewer</i> users, or with a host computer user. <i>VNC Viewer</i> users only. | YES | YES | |
| Connect without accept/reject prompt | Bypass connection prompts. For more information about this feature, see <i>Preventing particular users connecting</i> on page 108. | YES | | |

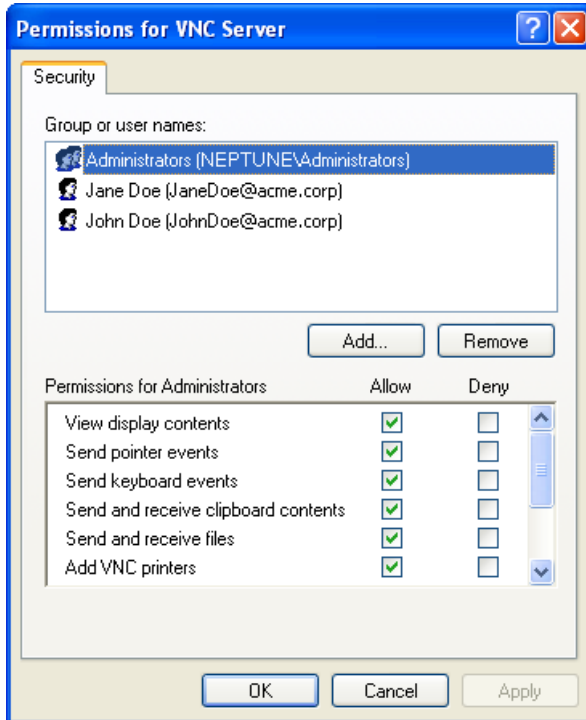
Customizing VNC permissions

If *VNC Server* specifies platform-native authentication or *Single sign-on* as its authentication mechanism, you can customize VNC permissions. For example, you might want to revoke permissions for a particular user in order to restrict their access to *VNC Enterprise Edition* functionality while connected. Note you cannot customize VNC permissions under any other authentication mechanism, or for users who bypass it.

Note: You can restrict access to *VNC Enterprise Edition* functionality for *all* connected users by configuring properties on the **Inputs** tab of the **VNC Server Properties** dialog. For more information, see *Restricting functionality for connected users* on page 90.

To customize VNC permissions, open the **VNC Server Properties** dialog. For more information on this dialog, see *Using the VNC Server Properties dialog* on page 85. On the **Connections** tab, click the

Configure button. Providing either `Windows password` (or equivalent) or `Single sign-on` is selected in the **Authentication** dropdown, the **Permissions for VNC Server** dialog opens:

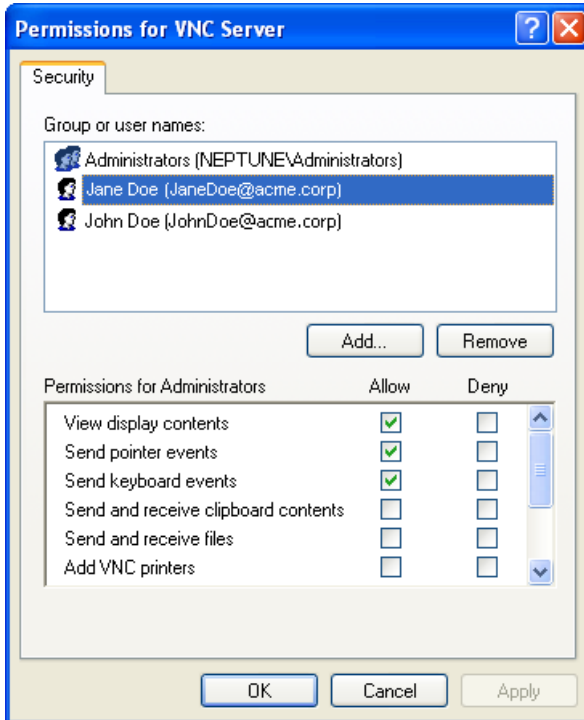


(Windows XP)

Note: A user can supply the credentials of any of the host computer users listed in **Group or user names** in order to connect to *VNC Server* (including any member of a group). To see how to configure host computer users or groups, see *Managing users and groups in the authentication list* on page 98.

You can change the VNC permissions allocated to a particular host computer user. To do this, select the appropriate entry in the **Group or user names** list, and turn individual permissions on or off. For example, in

the following dialog, just the `View display contents`, `Send pointer events`, and `Send keyboard events` permissions are turned on for the host computer user Jane Doe:



(Windows XP)

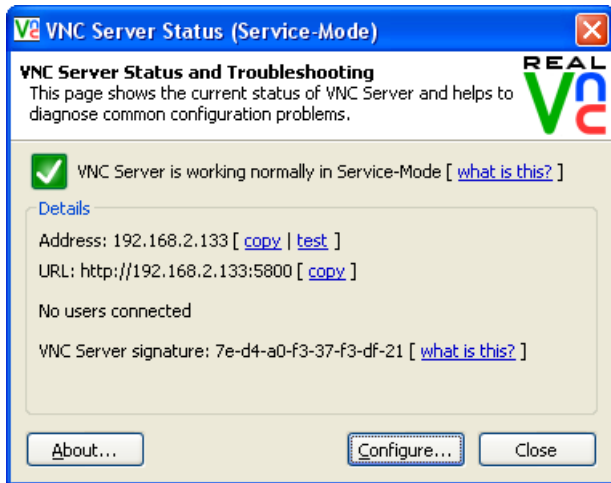
This means that any user supplying Jane Doe's credentials in order to connect to *VNC Server* is able to see the host computer's desktop, and control it using their keyboard and mouse. All other *VNC Enterprise Edition* functionality, however, is disabled. A connected user cannot copy and paste or bypass connection prompts and, if a *VNC Viewer* user, cannot print, chat, or transfer files.

Uniquely identifying VNC Server

VNC Server has a signature uniquely identifying it.

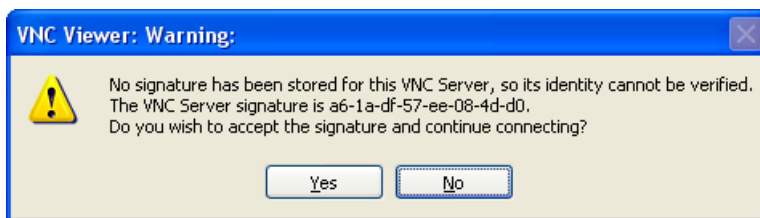
- Under Windows and Mac OS X, the signature uniquely identifies VNC Server among all instances running on the same host computer.
- Under UNIX or Linux, the signature is shared by instances of VNC Server started by the same host computer user.

A VNC Server signature is displayed in the **VNC Server Status** dialog:



(Windows XP)

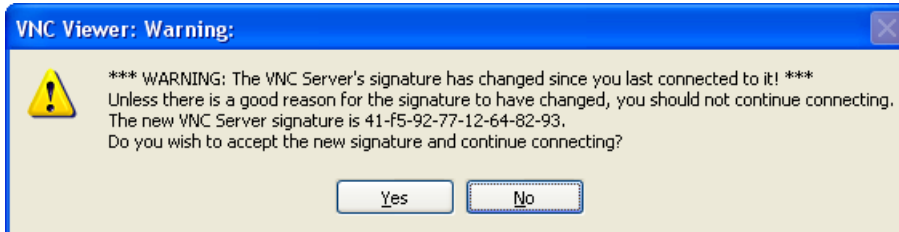
When a user connects from a particular client computer for the first time, this signature is published. The user is asked to verify it in order to continue connecting:



A connecting user may be able to check that the published signature matches that of VNC Server, for example if a host computer user is present, or if the connecting user set up VNC Server in the first place.

A VNC Server signature should not change. The next (and all subsequent) times a user connects from the same client computer, the signature is *not* published. If the signature changes, it may be because a third

party is interrupting the connection between client and host computers and eavesdropping on communications – a so-called ‘man-in-the-middle’ attack. If a user sees a message similar to the following:



then it is recommended that they do not continue connecting.

Note: The signature *does* change if *VNC Server* is re-installed on the host computer.

Upholding privacy

This section applies to host computers running Windows only.

By default, *VNC Enterprise Edition* promotes shared connections. That is to say, if more than one user is connected, all users can observe each other’s operations. In addition, if a host computer user is present while a connection is in progress, then that host computer user can observe the operations of connected users.

Under Windows, you can configure *VNC Server* to uphold the privacy of connected users by configuring various properties in the **VNC Server Properties** dialog. For more information on this dialog, see *Using the VNC Server Properties dialog* on page 85.

Note: A user can ensure their own privacy by disconnecting all other users when they connect. For more information, see *Configuring connections* on page 33.

Blanking the host computer’s monitor

You can blank the host computer’s monitor in order to prevent a host computer user observing the operations of connected users. To do this, turn on **Blank the screen while VNC Viewers are connected**. This property is on the **Desktop** tab.

Preventing input from the host computer

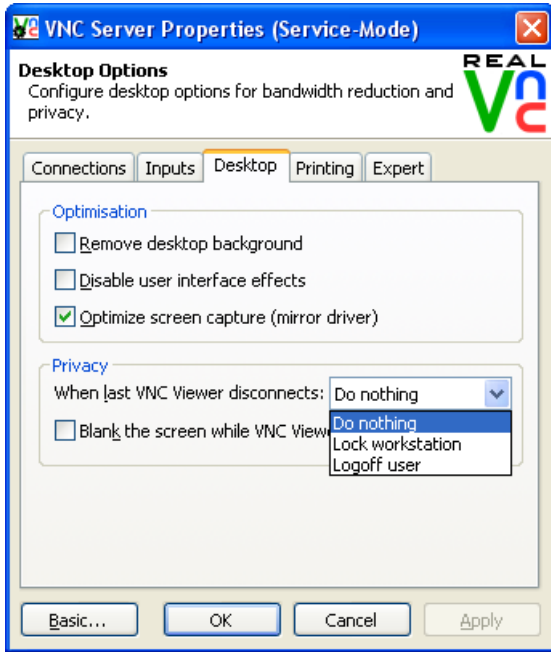
You can disable the keyboard and mouse of the host computer in order to prevent a host computer user interrupting the operations of connected users. To do this, turn on **Disable the keyboard and mouse while VNC Viewers are connected**. This property is on the **Inputs** tab.

Protecting the host computer

You can protect the host computer when no connections are in progress by locking it or logging off when the last user disconnects. Note that users connected to *VNC Server* in User Mode are disconnected, and cannot

reconnect. Users connected to VNC Server in Service Mode remain connected, but must know how to unlock the host computer or log back on in order to continue.

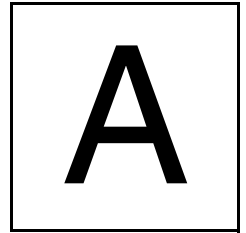
To do this, select an alternative to the default `Do nothing` option from the **When last VNC Viewer disconnects** dropdown on the **Desktop** tab:



(Windows XP)

To protect the host computer by:

- Locking the workstation, select `Lock workstation`.
- Logging off, select `Logoff user`. Note that VNC Server in User Mode will stop when the last user disconnects.



Saving Connections

This appendix explains how to save connections so you can quickly connect to favorite host computers again with just a few mouse clicks.

If you are using fully-featured *VNC Viewer*, you can save connections to *VNC Address Book*. *VNC Address Book* remembers network addresses, user names, and passwords (in encrypted form) so you do not have to, and automatically recreates your preferred *VNC Viewer* working environment each time you connect.

If you are using fully-featured or standalone *VNC Viewer*, you can save connections to icons on the client computer's desktop. You cannot save connections if you are connecting from a web browser.

Note: For more information on differences between *VNC Viewer* in different modes, see *VNC Enterprise Edition 4.5 connectivity* on page 12.

Contents

| | |
|---|-----|
| Saving connections to VNC Address Book | 118 |
| Using VNC Address Book to connect | 123 |
| Managing connections using VNC Address Book | 124 |
| Saving connections to desktop icons | 127 |

Saving connections to VNC Address Book

If you are using fully-featured *VNC Viewer*, you can save a connection to *VNC Address Book*. You can then use *VNC Address Book* instead of *VNC Viewer* to connect to the host computer in future.


Connecting from *VNC Address Book* means you do not have to remember the network address and port number of the host computer, nor your *VNC Server* user name and password. In addition, *VNC Address Book* automatically recreates your preferred *VNC Viewer* environment for controlling that computer, for example the scaling applied to the desktop, and the color quality.

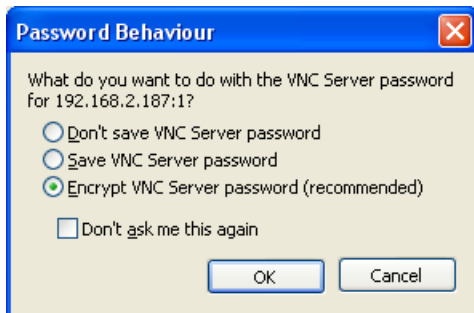
Note: Because *VNC Address Book* stores *VNC Server* authentication credentials, access to it is controlled by a *master password*. For more information on this, see *Working with the master password* on page 126.

You can use *VNC Address Book* to organize connections, configure the appearance and behavior of *VNC Viewer* for each one, and share connections with other *VNC Viewer* users.

Saving the current connection


If you are currently connected to a host computer using fully-featured *VNC Viewer*, you can save the connection to *VNC Address Book* while you work. To do this:

1. In *VNC Viewer*, click the **Save Connection**  toolbar button. *VNC Address Book* starts. If you entered a password in order to connect to *VNC Server*, you are prompted to save it:

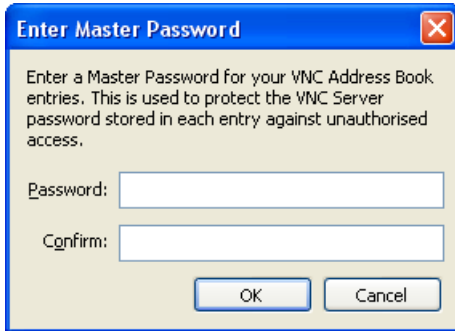


(Windows XP)

Choose:

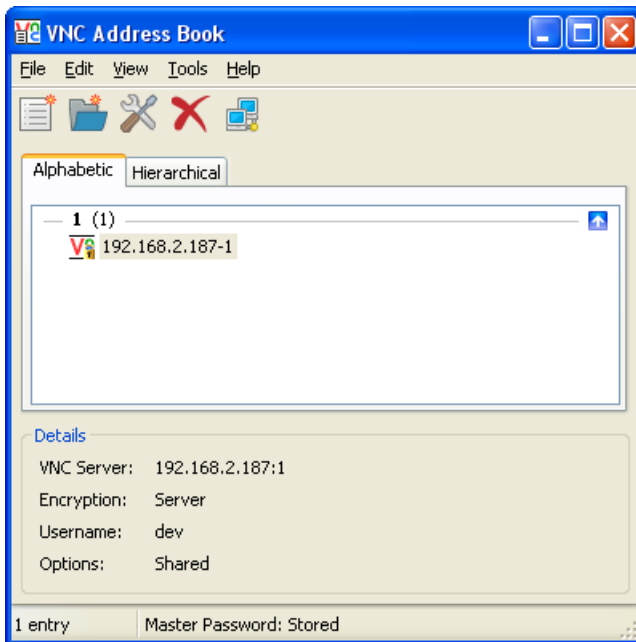
- **Don't save VNC Server password** to forget the password. You will need to enter it each time you connect using *VNC Address Book*.
- **Save VNC Server password** to save the password in obfuscated, though not encrypted, form. You will no longer need to remember the password. However, since the connection will not be protected by the *VNC Address Book* master password, any other user of your client computer will be able to connect.
- **Encrypt VNC Server password** to create a *protected connection* in which the password is both saved and encrypted. You will no longer need to remember it. You will, however, have to enter the *VNC Address Book* master password in order to connect, and also to configure the connection. Note that a protected connection is identified by a padlock symbol  throughout *VNC Address Book*.

- Click the **OK** button. If you chose to create a protected connection, and this is the first time you have used *VNC Address Book*, you are prompted to specify a master password:



(Windows XP)

- Click the **OK** button. The current connection is saved to *VNC Address Book*:



(Windows XP)

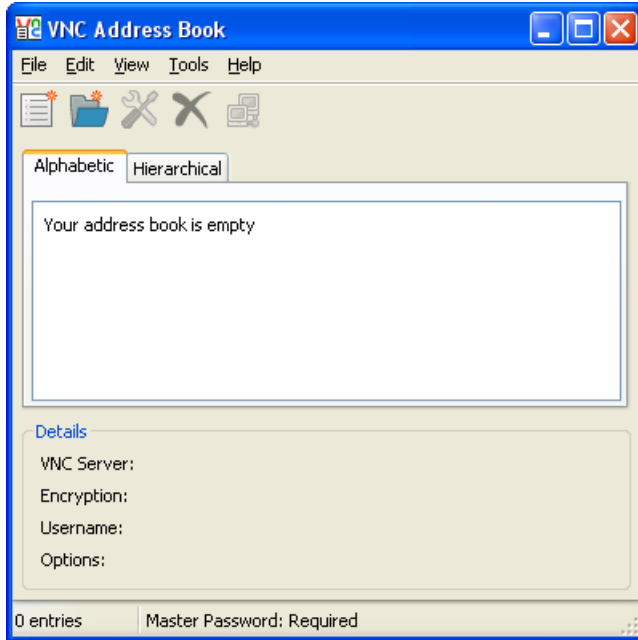
To see how to use *VNC Address Book* to connect to this host computer in future, read *Using VNC Address Book to connect* on page 123.

For more information on editing and organizing connections, start with *Organizing connections* on page 125.


Creating a new connection

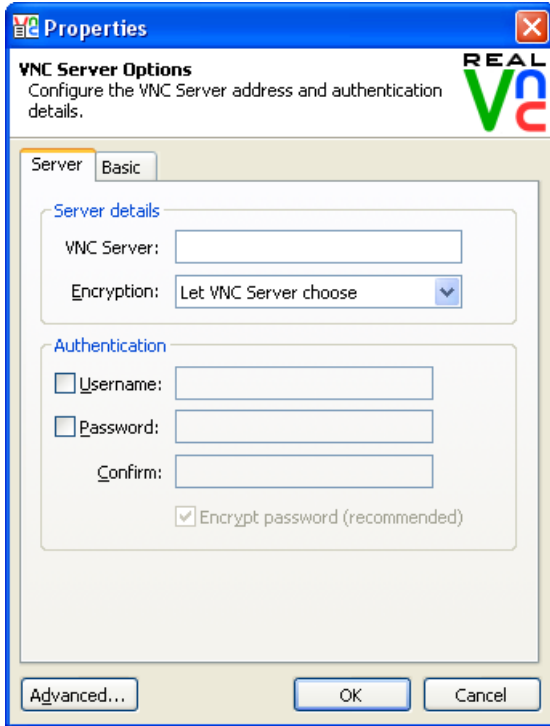
You can create a new connection in *VNC Address Book* directly. To do this:

1. Start *VNC Address Book* on the client computer. To see how to do this, read *Starting VNC Address Book* on page 124. The **VNC Address Book** dialog opens:




(Windows XP)

2. Click the **New Entry**  toolbar button. The **Properties** dialog opens:



(Windows XP)

3. Enter a network address for the host computer in the **VNC Server** field (including a port number if necessary), choose an **Encryption** option (or retain the default) and, optionally, specify your **VNC Server** user name and password in the **Authentication** area. To see how to find out this information, start with *Step 3: Identify VNC Server on the host computer* on page 17.

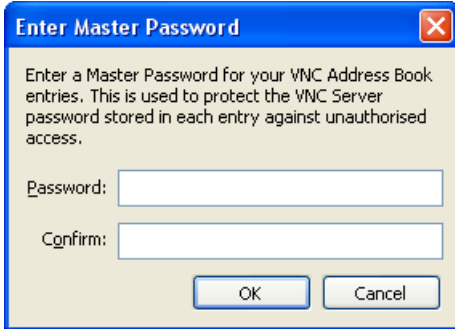
By default, *VNC Address Book* creates a *protected connection*. This means you must enter the *VNC Address Book* master password in order to connect to the host computer, and also to configure the connection. A protected connection is identified by a padlock symbol  throughout *VNC Address Book*.

Note: Turn off **Encrypt password (recommended)** if you do not want to enter the *VNC Address Book* master password in order to connect. Note this may constitute a security risk if others use your client computer.

You can optionally configure *VNC Viewer* properties to set up your preferred environment for controlling this host computer. To do this, use the **Basic** tab to configure common properties, or click the **Advanced** button to see all the tabs. For more information, start with *Configuring VNC Viewer before you connect* on page 31.

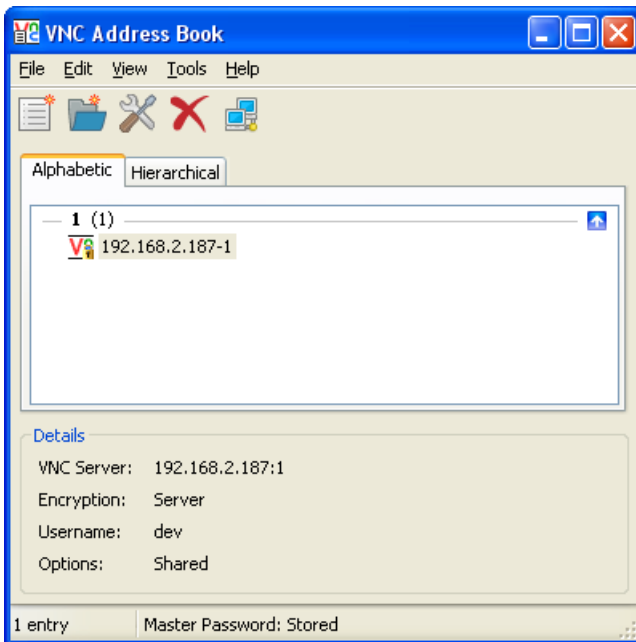
Appendix A: Saving Connections

4. Click the **OK** button. If you chose to create a protected connection, and this is the first time you have used *VNC Address Book*, you are prompted to specify a master password:



(Windows XP)

5. Click the **OK** button. The connection is saved to *VNC Address Book*:



(Windows XP)

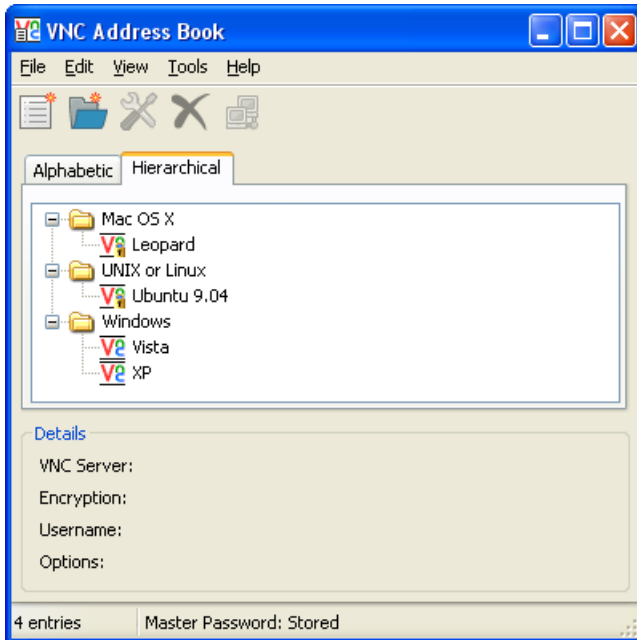
To see how to use *VNC Address Book* to connect to this host computer, read *Using VNC Address Book to connect* on page 123.

For more information on editing and organizing connections, start with *Organizing connections* on page 125.


Using VNC Address Book to connect

You can quickly connect to a host computer using *VNC Address Book*. To do this:


1. Start *VNC Address Book* on the client computer. To see how to do this, read *Starting VNC Address Book* on page 124. The **VNC Address Book** dialog opens:



(Windows XP)

2. Either:
 - Double-click a connection in the **Alphabetic** or **Hierarchical** tab list.
 - Select a connection in either list and click the **Connect**  toolbar button.

You may be required to enter the *VNC Address Book* master password in order to connect. For more information, see *Working with the master password* on page 126.

Under Windows, when *VNC Address Book* starts, a *VNC Address Book* icon  is displayed in the Notification area. This icon provides further options for quickly and conveniently connecting to host computers. For more information, see *Working with VNC Address Book* on page 124.

Managing connections using VNC Address Book


This section explains *VNC Address Book* features and operations.

Starting VNC Address Book

To start *VNC Address Book*:

- Under Windows, select **RealVNC > VNC Address Book** from the **Start** menu.
Note: Under Windows, you can start *VNC Address Book* automatically when the computer is powered on. To do this, select **Edit > Options** and, in the **UI behavior** area, turn on **Start with Windows**.
- Under UNIX or Linux, either type `vncaddrbook` in a Terminal window and press the ENTER key, or select **Applications > Internet > VNC Address Book** from the menu system, if available.
- Under Mac OS X, navigate to the **Applications > RealVNC** folder, and double-click the **VNC Address Book** program.

Working with VNC Address Book

Under Windows, while *VNC Address Book* is running, a *VNC Address Book* icon  is displayed in the Notification area:

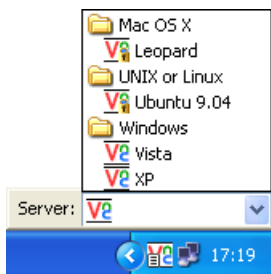


(Windows XP)

Note: Under UNIX or Linux and Mac OS X, no *VNC Address Book* icon is available. However, all the operations explained below can be performed from the **VNC Address Book** dialog.

The *VNC Address Book* icon:

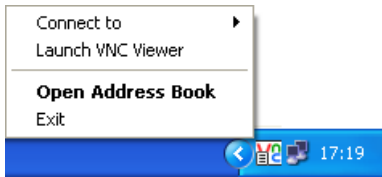
- Provides visual confirmation that *VNC Address Book* is running on the client computer. If the icon is not visible (and not hidden by other icons), then *VNC Address Book* is not running.
- Has a quick launch bar enabling you to select a host computer to connect to:



(Windows XP)

To open the quick launch bar, click the *VNC Address Book* icon.

- Has a right-click shortcut menu that performs useful operations:



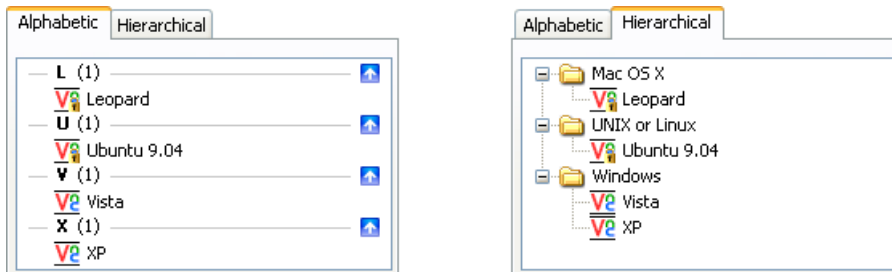
(Windows XP)

The following table explains the effect of selecting each *VNC Address Book* shortcut menu option.

| Shortcut menu option | Explanation |
|----------------------|--|
| Connect to | Opens a menu where you can select a host computer to connect to. |
| Launch VNC Viewer | Starts <i>VNC Viewer</i> , enabling you to connect to a new host computer in the standard way. For more information, see <i>Connecting to a host computer</i> on page 35. |
| Open Address Book | Opens the VNC Address Book dialog, enabling you to create new connections or edit and organize existing ones. (Alternatively, double-click the <i>VNC Address Book</i> icon.) |
| Exit | Closes <i>VNC Address Book</i> . |


Organizing connections

VNC Address Book organizes connections both alphabetically and hierarchically:



(Windows XP)

You can reorganize connections in the **Hierarchical** tab list. (The **Alphabetic** tab list is automatically maintained.)

Click the **New Folder**  toolbar button to create folders in the **Hierarchical** tab list. You can drag-and-drop connections to, from, and between folders. Note that if you delete a folder, all connections in that folder are deleted too.

Editing connections

You can edit an existing connection. Note you may first be required to enter the *VNC Address Book* master password.

To do this, select a connection in the **Alphabetic** or **Hierarchical** tab list, and either:

- Click the **Properties**  toolbar button.
- Select **Edit > Properties**.

For more information on editing *VNC Viewer* properties, start with *Configuring VNC Viewer before you connect* on page 31.

To rename a connection in *VNC Address Book*, select it in the **Alphabetic** or **Hierarchical** tab list and select **Edit > Rename**, or right-click and select **Rename** from the shortcut menu.

Sharing connections

You can share one or more connections with other fully-featured *VNC Viewer* users. Note that *VNC Server* passwords are also shared, albeit in obfuscated or encrypted form.

To share:

- All *VNC Address Book* connections, select **Tools > Export Address Book**.
- A single connection, right-click it in the **Alphabetic** or **Hierarchical** tab list and, from the shortcut menu, select **Export**.

Choose a location for the exported file. If the file contains a protected connection (one in which the *VNC Server* password was saved and encrypted), the recipient will need your *VNC Address Book* master password in order to import it.

You can import one or more connections shared by other fully-featured *VNC Viewer* users. To do this, select **Tools > Import Address Book**, and select the file to import. If the file contains a protected connection, you will need the *VNC Address Book* master password of the user who created the file in order to import it.

Removing connections

To remove a connection, select it in the **Alphabetical** or **Hierarchical** tab list, and either:

- Click the **Delete**  toolbar button.
- Select **Edit > Delete**.

Working with the master password

If you chose to encrypt a *VNC Server* password when you saved a connection to a host computer, you created a *protected connection*.

VNC Address Book secures protected connections using the *master password*. You must enter the master password in order to perform an operation on a protected connection, for example connecting to the host computer, or configuring connection details or *VNC Viewer* properties.

Note: You do not have to enter the master password in order to perform operations on connections for which the *VNC Server* password was not saved, or was saved in obfuscated, though not encrypted, form. For more information on saving *VNC Server* passwords, start with *Saving the current connection* on page 118.

By default, *VNC Address Book* remembers the master password for one hour. This means you do not have to enter it for sixty minutes after you first enter it in order to perform an operation on a protected connection. To change this, and require the entry of the master password, select:

- **Tools > Forget Master Password** to require the entry of the master password for the *next* operation on a protected connection.
- **Tools > Options** and, in the **Master password** area, turn off **Remember for** to require the entry of the master password for all future operations on protected connections. (Alternatively, you can decrease the length of time the master password is remembered.)

Note: The Status Bar reports `Master Password: Stored` if you do not currently need to enter the master password, and `Master Password: Required` if you do.

To change the master password, select **Tools > Options** and, in the **Master password** area, click the **Change** button.

Saving connections to desktop icons

If you are using either fully-featured or standalone *VNC Viewer*, you can save the current connection to a desktop icon on the client computer:





(Windows XP)

A desktop icon provides an extremely quick and convenient way of connecting to a host computer. Simply double-click the icon to connect. Your preferred *VNC Viewer* environment for controlling the host computer is automatically recreated.

Note: For standalone *VNC Viewer*, you may need to associate the icon with the *VNC Viewer* executable file the first time you connect.

To save the current connection as a desktop icon:

1. In *VNC Viewer*, click the **Save Connection**  toolbar button.

Note: For fully-featured *VNC Viewer*, you must first disable *VNC Address Book*. To do this, click the **Options**  toolbar button to open the **VNC Viewer Properties** dialog and, on the **Expert** tab, set the **UseAddrBook** property to `False`.
2. If you entered a password in order to connect to *VNC Server*, you are prompted to save the password. Note that doing so may constitute a security risk, since the password is saved in obfuscated, though not encrypted, form. If you do not save the password, you must enter it each time you connect.
3. Choose a location to save the icon file to (for example, the desktop), and an intuitive name.

Appendix A: Saving Connections