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, 2010-2011. 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’s 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
Appendix A: Saving Connections 115

Saving connections to VNC Address Book 116
Using VNC Address Book to connect 121
Managing connections using VNC Address Book 122
Saving connections to desktop icons 125
About This Guide

This User Guide explains how to use VNC Enterprise Edition 4.6 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 4.6 with the exception of sections on system authentication, and to VNC Viewer Plus 1.x for connections 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.
• Chapters 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

Visit www.realvnc.com for:

• Supported platforms, operating systems, and system requirements.
• Instructions on how to install, license, and uninstall VNC Enterprise Edition, and getting a trial license key.
• Release Notes and FAQs.
• Related program downloads.
• 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.
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 for 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 system authentication, and to VNC Viewer Plus for connections to VNC Server.

Contents

- What is VNC Enterprise Edition? 10
- Getting VNC Enterprise Edition ready to use 10
- VNC Enterprise Edition 4.6 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 they 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.

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, 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, visit the installation and licensing documentation appropriate to the platform of the host computer at www.realvnc.com/products/enterprise/4.6.

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 the credentials for such a user are not available, change the default authentication mechanism. See Authenticating connections to VNC Server on page 92 for more information.

Note: If you cannot perform these operations and a host computer user is present, you may be able to jointly perform a reverse connection. See Establishing a reverse connection on page 102 for more information.

Client computer

1. Ensure your 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.
Chapter 1: Introducing VNC Enterprise Edition

For detailed instructions, visit the installation documentation appropriate to the platform of the client computer at www.realvnc.com/products/enterprise/4.6. Note you do not need a license to use VNC Viewer.

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.

3. If your client computer is protected by a proxy server, specify the details of that proxy server. For more information, see Connecting via a proxy server on page 32.

VNC Enterprise Edition 4.6 connectivity

Unless stated, this User Guide assumes you are connecting from a client computer running fully-featured VNC Viewer 4.6 to a host computer running VNC Server 4.6.

Connecting to a different VNC Server

You can use VNC Viewer 4.6 to connect to:

• A version of VNC Server prior to 4.6.
• A computer running VNC Personal Edition or VNC Free Edition.
• A Mac OS X computer with built-in Apple Remote Desktop or Remote Management enabled (to do this, turn on VNC viewers may control screen with password, and set a password).
• VNC-compatible Server software from a third party.

Note that not all the functionality of VNC Enterprise Edition 4.6 is available in these circumstances. In particular, you cannot:

• Encrypt connections to VNC Free Edition, Apple Remote Desktop/Remote Management, or VNC-compatible Server software. In fact, you must turn encryption off in order to connect at all.
• Print host computer files unless the host computer is running at least VNC Server 4.5. Even then, VNC Viewer 4.6 for Windows cannot print host computer files from VNC Server 4.5 for Unix or Linux or Mac OS X.
• Transfer files from VNC Server 4.5 for Windows in Service Mode to VNC Viewer 4.6 for UNIX or Linux or Mac OS X. You can start VNC Server 4.5 for Windows in User Mode on the host computer and transfer files using that instead.

Connecting from a different VNC Viewer

You can connect to VNC Server 4.6 from:

• A version of fully-featured VNC Viewer prior to 4.6.
• Standalone VNC Viewer.
• A Java-enabled web browser.

Note that not all the functionality of VNC Enterprise Edition 4.6 is available in these circumstances. See the sections below for more information.
Connecting from an earlier version of VNC Viewer

You can connect to VNC Server 4.6 from a version of VNC Viewer prior to 4.6, but note that certain features will not be available. In particular, you cannot:

- Encrypt connections using 256-bit AES.
- Print host computer files (from VNC Viewer 4.4 or earlier).
- 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 (from VNC Viewer 4.4 or earlier).
- Chat with other connected users, or with a host computer user, on computers running UNIX or Linux or Mac OS X (from VNC Viewer 4.4 or earlier).

Note that 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 4.6 from standalone VNC Viewer 4.6. This application is freely available to download and run for any supported platform from the RealVNC web site.

Note that if you use standalone VNC Viewer, you cannot save connections to VNC Address Book. You can still save connections to desktop icons.

Connecting from a web browser

You can connect to VNC Server 4.6 from a Java-enabled web browser. For more information, see Chapter 4, Connecting From A Web Browser on page 47. 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 the 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, and you may be sharing the host computer’s desktop—and therefore control—with other users.) Or you may be sitting in front of a host computer and need to know how to set up VNC Server for multiple incoming connections. 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 establishing your first connection from a client computer running VNC Viewer to a host computer running VNC Server, see Chapter 2, Getting Connected 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 47.
- To see how to exchange information between client and host computers, read Chapter 5, Exchanging Information on page 57.
- 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 69.
- 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, Securing Connections on page 91.
Getting Connected

This chapter aims to help the majority of users get started establishing their first connection from a client computer running VNC Viewer to a host computer running VNC Server. For more detailed connection information, read Chapter 3, Using VNC Viewer on page 29.

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 and the host computer 17
- Step 4: Request 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. Note you should not be a user with administrative privileges when you run this command.
  - 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.

The VNC Server 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 dialog opens:

![VNC Viewer dialog](Windows XP)

Step 3: Identify VNC Server and 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 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]`. (Note 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 the router, see Connecting over the Internet on page 22.
Chapter 2: Getting Connected

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: Request 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: Request an encryption option

VNC Enterprise Edition is designed to be completely secure. By default, all communication between client and host computer is encrypted using industry-standard 128-bit AES. For more information on security, see Chapter 7, Securing Connections on page 91.

By default, in the VNC Viewer 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 either to request that:

• Encryption be turned off.
• The AES key size be increased to 256-bit for maximum security.

For more information on either operation, see Changing the encryption rules on page 103.

Note: Encryption requests are managed 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.

Step 5: Connect and authenticate to VNC Server

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

(Windows XP)
Chapter 2: Getting Connected

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

![VNC Viewer](image)

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 dialog:

![VNC Server signature](image)

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 112.

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

![Authentication Credentials](image)

(Windows XP)

If so, enter the credentials of a user with administrative privileges on the host computer. Note that if you:

- Do not know such credentials but have access to the host computer, you may be able to find them 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), then you must change the default authentication mechanism, or disable authentication altogether.

For more information, start with Authenticating connections to VNC Server on page 92. If you do not have access to the host computer, 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 The VNC Viewer user experience on page 34.

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 115.
Troubleshooting connection

This section provides 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 102.

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 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 the host computer, follow the appropriate instructions for its 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)
Chapter 2: Getting Connected

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, over a cellular network, or in to the office on the move), it is very 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 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 either to follow the instructions below, or visit 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 dialog.
2. In the Details area, click the [test] link:

   ![Details](image)

   The 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:

   ![Connection Test](image)

   (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 212.44.6.81.
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: 212.44.6.81. In addition, to connect to host computer C, you must qualify the router’s network address with the port number: 212.44.6.81:1. 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 83.

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:

\[
\text{johndoe:1} \\
192.168.2.187:1 \\
[2001:db8::1]:1
\]

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:

\[
\text{johndoe::6001} \\
192.168.2.187::6001 \\
[2001:db8::1]::6001
\]

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 dialog. If applicable, this information is appended to the network address in the Details area:

```
Details
Address: 192.168.2.183:80
```

In this example, VNC Server is running on host computer 192.168.2.183 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 dialog. If applicable, this information is appended to the network address in the Details area:

```
Details
Address: 192.168.2.107:1
```

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 dialog. If applicable, this information is appended to the network address in the Details area:

```
Details
Address: 192.168.2.168:6001
```

In this example, VNC Server is running on host computer 192.168.2.168 and listening on port 6001.
Chapter 2: Getting Connected

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:

![Error message](image)

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 messages you might see.

Failing to authenticate correctly

If you see the following error message:

![Error message](image)

then you have not authenticated yourself correctly to VNC Server. Note that user names and passwords are case-sensitive.

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 97.
Failing to authenticate as ‘you’

If you see the following error message:

![VNC Viewer error message](image)

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 96.

Connecting from an unauthorized computer

If you see the following error message:

![VNC Viewer error message](image)

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 105.

Alternatively, you may be able to connect from a different client computer.
Chapter 2: Getting Connected

Being rejected by a host computer user

If you see the following error message:

![VNC Viewer]

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 107.
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 4.6 connectivity* on page 12.

### Contents

- Starting VNC Viewer 30
- Starting Listening VNC Viewer 30
- Configuring VNC Viewer before you connect 31
- Connecting to a host computer 33
- The VNC Viewer user experience 34
- Using the toolbar 36
- Using the shortcut menu 38
- Using the Options dialog 39
- Managing the current connection 40
- Changing appearance and behavior 41
- Restricting access to functionality 43
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 Applications > RealVNC, and double-click the VNC Viewer program.

The VNC Viewer dialog opens:

(VNC Viewer dialog shown)

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

To carry on connecting, see Connecting to a host computer on page 33.

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 102.

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 Applications > RealVNC > Advanced, and double-click the Start Listening VNC Viewer program.
Under Windows and Mac OS X, a VNC Viewer icon \[\text{VNC Viewer}\] is displayed in the Notification area and Status bar respectively. Hover the mouse cursor over the icon to confirm that Listening VNC Viewer is running:

\[
\text{Listening VNC Viewer} \quad \text{12:09}
\]

(Windows XP)

Under Windows and Mac OS X, Listening VNC Viewer has a shortcut menu:

\[
\begin{array}{|l|}
\hline
\text{New Connection...} \\
\text{Default Options...} \\
\text{About...} \\
\text{Close} \\
\hline
\end{array}
\]

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

Note you can select New Connection to use VNC Viewer to establish a connection to VNC Server in the normal way. Carry on from Connecting to a host computer on page 33.

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 The VNC Viewer user experience on page 34.
- Is not successful, start with Establishing a reverse connection on page 102.

## Configuring VNC Viewer before you connect

In most circumstances, VNC Viewer is ready to connect to VNC Server out-of-the-box. You do not need to configure it. However, the following exceptions apply:

- Your client computer is protected by a proxy server. See Connecting via a proxy server on page 32.
- You want to disconnect other users so you can control the host computer alone. See Disconnecting other users on page 33.
- VNC Server specifies single sign-on but you do not want to connect as the user you logged on as. See Disabling single sign-on on page 33.
- You want to specify printing options. See Configuring printing on page 33.
To configure VNC Viewer before you connect, click the Options button at the bottom of the VNC Viewer dialog (see Starting VNC Viewer on page 30 for more information). The Options dialog opens:

![Options dialog](image)

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

For more information on this dialog, see Using the Options dialog on page 39. Note that the Connection and Printing tabs are not available after you connect.

**Connecting via a proxy server**

If your client computer is protected by a proxy server, you must tell VNC Viewer about that proxy server. On the Connection tab, choose:

- **Use Microsoft Internet Explorer proxy settings** if this browser has already been provisioned with proxy server information. Note this option has a different name under UNIX or Linux and Mac OS X.
- **Use these proxy settings** to specify the network address of either an HTTP or a SOCKS 5 proxy server, and a port on which an appropriate application or process is listening, separated by a colon.

**Note:** Proxy servers that require authentication are not supported. This may be the subject of a future release.
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) on the Connection tab. Note that you may be disconnected in turn.

Disabling single sign-on

Note: The information in this section applies to 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 to a network when logging on to your client computer. For more information, see Relaxing the authentication rules on page 97.

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 on the Connection tab. You will need to know the user name and password of a valid host computer user.

Configuring printing

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 58.

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 on the Printing tab.

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 Connected on page 15.

1. Start VNC Viewer on the client computer. The VNC Viewer 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 to VNC Server.
Chapter 3: Using VNC Viewer

If the connection is successful, VNC Viewer displays the host computer’s desktop in a new window on the client computer. Carry on from The VNC Viewer user experience on page 34. 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 115.

The VNC Viewer user 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 33.

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 visible to a host computer user. For more information on this feature, see Running multiple instances of VNC Server on page 74.

Note that 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!

Controlling the host computer using your mouse

Your client computer's mouse is 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.

Note: If your mouse has no effect on the host computer, it may have been disabled. For more information, see Restricting access to functionality on page 43.

If client and host computers have different numbers of mouse buttons, you can configure VNC Viewer to emulate those you do not have. See Configuring your mouse on page 42 for more information.

Controlling the host computer using your keyboard

Your client computer's keyboard is now shared with the host computer, with the exception of:

- The function key that opens the shortcut menu (F8 by default).
- The CTRL-ALT-DELETE key combination.

These commands are interpreted by the client computer. Alternative ways of sending them to the host computer are available; start with Using the shortcut menu on page 38 for more information.

Under Windows, note you can choose for certain other keys or key combinations to be interpreted by your client computer rather than the host. See Configuring your keyboard on page 42 for more information.

Note: If your keyboard has no effect on the host computer, it may have been disabled. For more information, see Restricting access to functionality on page 43.

Note it is possible for 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 Mac OS X from Windows or Linux with a PC keyboard, or vice versa; see www.realvnc.com/products/enterprise/4.6/mac.html for more information.
Chapter 3: Using VNC Viewer

Interacting with VNC Server

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

![VNC Server Icon](Windows XP client computer, Ubuntu 8.10 Linux host)

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 77.

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. In the latter scenario, shortcut menu commands are available from a Commands button on the VNC Server dialog.

Note that the VNC Server icon also provides access to VNC Server options. 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 92.

Using the 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 appearance and behavior on page 41.

The VNC Viewer toolbar is located at the top center of the VNC Viewer window. To use it, hover the mouse cursor over the hot area:

![VNC Viewer Toolbar](Windows XP)

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

<table>
<thead>
<tr>
<th>Button name</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="icon" alt="New Connection" /></td>
<td>Opens the VNC Viewer dialog. You can establish a new connection to the same host computer, or to a different one. Carry on from Connecting to a host computer on page 33.</td>
</tr>
<tr>
<td><img src="icon" alt="Save Connection" /></td>
<td>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 Appendix A, Saving Connections on page 115.</td>
</tr>
</tbody>
</table>
## Chapter 3: Using VNC Viewer

<table>
<thead>
<tr>
<th>Button name</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Close Connection</td>
<td>Prompts you to close the current connection (and the VNC Viewer window).</td>
</tr>
<tr>
<td>Options</td>
<td>Opens the <strong>Options</strong> dialog. You can configure most aspects of VNC Viewer while the current connection is in progress. For more information, see Using the Options dialog on page 39. Note that some options must be configured before you connect. For more information, see Configuring VNC Viewer before you connect on page 31.</td>
</tr>
<tr>
<td>Full Screen Mode</td>
<td>Toggles full screen mode on and off.</td>
</tr>
<tr>
<td>Send Ctrl-Alt-Del</td>
<td>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.</td>
</tr>
<tr>
<td>File Transfer</td>
<td>Opens a dialog where you can browse to the location of client computer files to send to the host computer. For more information, see Transferring files between client and host computers on page 60.</td>
</tr>
<tr>
<td>Start Chat Session</td>
<td>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 Communicating securely using chat on page 65.</td>
</tr>
<tr>
<td>Connection Information</td>
<td>Opens a dialog displaying technical information about the current connection, such as the encryption method and compression format.</td>
</tr>
<tr>
<td>encryption</td>
<td>The connection is encrypted/not encrypted. (Only one of these buttons is shown.)</td>
</tr>
<tr>
<td>connection speed/activity</td>
<td>Hovering over this toolbar button reveals the current connection speed. For more information on performance, see Changing appearance and behavior on page 41.</td>
</tr>
</tbody>
</table>
Chapter 3: Using VNC Viewer

Using the 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 toolbar on page 36.

Note: If you cannot access the VNC Viewer shortcut menu, it may have been disabled. For more information, see Changing appearance and behavior on page 41.

By default, to open the shortcut menu, press the F8 key (you may need to hold down the FN key on some PC laptops or Mac OS X computers):

<table>
<thead>
<tr>
<th>X Close</th>
<th>Alt+F4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exit Screen</td>
<td>Relative Pointer Motion</td>
</tr>
<tr>
<td>Send F8</td>
<td>Send Ctrl-Alt-Delete</td>
</tr>
<tr>
<td>Ctrl key</td>
<td>Alt key</td>
</tr>
<tr>
<td>Refresh Screen</td>
<td></td>
</tr>
<tr>
<td>Open Connection...</td>
<td>New Connection...</td>
</tr>
<tr>
<td>Options...</td>
<td>Connection Info...</td>
</tr>
<tr>
<td>About VNC Viewer...</td>
<td></td>
</tr>
<tr>
<td>File Transfer...</td>
<td>Start chat session...</td>
</tr>
</tbody>
</table>

(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.

<table>
<thead>
<tr>
<th>Shortcut menu option</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relative Pointer Motion</td>
<td>Turn this option on if the host computer's mouse cursor appears to be behaving abnormally, for example by accelerating too fast.</td>
</tr>
<tr>
<td>Send F8</td>
<td>Sends an F8 command to the host computer. (By default, F8 opens the shortcut menu; see Changing the shortcut menu key on page 43 for how to choose a different key.)</td>
</tr>
<tr>
<td>Ctrl key</td>
<td>Turn this option on to simulate holding down the CTRL key.</td>
</tr>
<tr>
<td>Alt key</td>
<td>Turn this option on to simulate holding down the ALT key.</td>
</tr>
<tr>
<td>Refresh Screen</td>
<td>Refreshes the display of the host computer's desktop.</td>
</tr>
<tr>
<td>About VNC Viewer</td>
<td>Displays version information. You may need this if you contact Support.</td>
</tr>
</tbody>
</table>
Chapter 3: Using VNC Viewer

Using the Options dialog

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

![Options dialog](image)

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

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

To open the Options 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 appearance and behavior on page 41.)

The first time you open this dialog, it opens in Basic mode, and only one tab is available, containing the most common options. 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 options 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 toolbar* on page 36.

**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 authentication credentials. In addition, your preferred VNC Viewer environment for controlling the host computer is automatically recreated each time.

To save the current connection, click the *Save Connection* toolbar button. Carry on from *Appendix A, Saving Connections* on page 115.

**Establishing a new connection**

You can establish 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 dialog opens. Carry on from *Connecting to a host computer* on page 33.

By default, any options you configure are inherited by the new connection. To prevent this, open the *Options* dialog and turn off *Use these settings for all new connections* first. For more information on this dialog, see *Using the Options dialog* on page 39.

**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 appearance and behavior

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.
- The **VNC Viewer** window is set to a particular size.
- **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** toolbar is accessible (from the top center hot area).
- The **VNC Viewer** shortcut menu is accessible (by pressing F8).

You can change these defaults by configuring options on the **Display** tab of the **Options** dialog. For more information on this dialog, see **Using the Options dialog** on page 39.
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 the desktop to a custom size, choose Custom scaling, and specify a width and height. Turn on Preserve aspect ratio to automatically calculate a height for a given width, and vice versa. Note that the VNC Viewer window inherits these dimensions and cannot be made bigger using the mouse, only smaller.

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 toolbar button.

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.

Conversely, you may be able to improve the picture quality by increasing the number of colors. To do this, move the slider towards Best quality. Note that sending more pixel information across the network may have an adverse effect on performance.

Configuring your mouse

Note: The information in this section applies to VNC Viewer for Windows and Mac OS X only.

You can emulate buttons missing because your mouse has fewer buttons than the host computer’s mouse. For example, if your mouse only has two buttons, 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, if your mouse only has one button, 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 options are on the Inputs tab.

Configuring your keyboard

Note: The information in this section applies to VNC Viewer for 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 option is on the Inputs tab.

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

You can disable the VNC Viewer toolbar. For more information on this toolbar, see Using the toolbar on page 36. 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 shortcut menu

You can disable the VNC Viewer shortcut menu. For more information on this menu, see Using the shortcut menu on page 38. To do this, select none from the Menu key dropdown. Note this option 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 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 option 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 88. 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 options on the Inputs tab of the Options dialog. For more information on this dialog, see Using
Chapter 3: Using VNC Viewer

The Options dialog on page 39. You might want to do this if you are watching a demonstration on the host computer, for example, and want to prevent inadvertent interruption.

(Windows XP)

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 appearance and behavior on page 41.

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 60.

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 64.

Disabling chat
You can disable chat. To do this, turn off Enable chat. For more information about this feature, see Communicating securely using chat on page 65.
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 the functionality of VNC Viewer is available.

Note: For more on differences with VNC Viewer, start with VNC Enterprise Edition 4.6 connectivity on page 12.

Contents

Connecting to a host computer 48
The VNC Viewer for Java user experience 52
Working with VNC Viewer for Java 53
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. Java (JRE or JDK) 5 or later is required.

2. In the address 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, and you are connecting within a private network, the information you need is displayed on the VNC Server dialog, marked URL:

For more information on this dialog, see Using the VNC Server dialog on page 79. If you are connecting over the Internet, you will probably need to enter the network address of a router instead. See Connecting over the Internet on page 22 for more information.

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 more 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 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 dialog opens:

(Windows XP. The web browser is Internet Explorer 8.)
Chapter 4: Connecting From A Web Browser

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 process as connecting from VNC Viewer.

By default, the VNC Server dropdown on the VNC Viewer 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):

![VNC Viewer](image)

(Windows XP)

For more information on network addresses and port numbers, start with Step 3: Identify VNC Server and 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: Request 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 51.

3. Click the Connect button.

You may be asked to confirm a signature that uniquely identifies VNC Server, and to authenticate. 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 The VNC Viewer for Java user experience on page 52.

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 options 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 Options dialog on page 54.

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

(Windows XP)

The following options 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 option 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 option is on the Misc tab.
Chapter 4: Connecting From A Web Browser

The VNC Viewer for Java user 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 10.04 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 mouse on page 35.
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):

<table>
<thead>
<tr>
<th>Shortcut menu option</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exit VNC Viewer</td>
<td>Closes VNC Viewer for Java.</td>
</tr>
<tr>
<td>Clipboard...</td>
<td>-------------</td>
</tr>
<tr>
<td>Send F8</td>
<td>Sends an F8 command to the host computer. (F8 opens the shortcut menu.)</td>
</tr>
<tr>
<td>Refresh screen</td>
<td>-------------</td>
</tr>
<tr>
<td>New connection...</td>
<td>-------------</td>
</tr>
<tr>
<td>Options...</td>
<td>-------------</td>
</tr>
<tr>
<td>Connection info...</td>
<td>-------------</td>
</tr>
<tr>
<td>About VNC Viewer...</td>
<td>-------------</td>
</tr>
<tr>
<td>Dismiss menu</td>
<td>-------------</td>
</tr>
</tbody>
</table>

(Windows XP)

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

<table>
<thead>
<tr>
<th>Shortcut menu option</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exit VNC Viewer</td>
<td>Closes VNC Viewer for Java.</td>
</tr>
<tr>
<td>Clipboard</td>
<td>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 Copying and pasting on page 55. Note that if you chose not to trust VNC Viewer for Java when you downloaded it, you can only copy and paste text between the two computers via this dialog.</td>
</tr>
<tr>
<td>Send F8</td>
<td>Sends an F8 command to the host computer. (F8 opens the shortcut menu.)</td>
</tr>
</tbody>
</table>
Chapter 4: Connecting From A Web Browser

Using the Options dialog

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

<table>
<thead>
<tr>
<th>Shortcut menu option</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Ctrl-Alt-Del</td>
<td>Sends the CTRL-ALT-DELETE command to the host computer. (Pressing this key combination would be interpreted by the client computer.)</td>
</tr>
<tr>
<td>Refresh screen</td>
<td>Refreshes the display of the host computer's desktop.</td>
</tr>
<tr>
<td>New connection</td>
<td>Opens the VNC Viewer 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 VNC Viewer for Java again. For more information, see Connecting to VNC Server on page 50.</td>
</tr>
<tr>
<td>Options</td>
<td>Opens the Options dialog. You can configure most aspects of VNC Viewer for Java while the current connection is in progress. For more information, see Using the Options dialog on page 54. Note that some options must be configured before you connect. For more information, see Configuring VNC Viewer for Java before you connect on page 51.</td>
</tr>
<tr>
<td>Connection info</td>
<td>Opens a dialog displaying technical information about the current connection, such as the encryption method and compression format.</td>
</tr>
<tr>
<td>About VNC Viewer</td>
<td>Displays information about VNC Viewer for Java.</td>
</tr>
<tr>
<td>Dismiss menu</td>
<td>Closes the shortcut menu.</td>
</tr>
</tbody>
</table>

Note: Some VNC Viewer for Java options must be configured before you connect. For more information, see Configuring VNC Viewer for Java before you connect on page 51.

To open the 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 53.

The following sections explain the options in this dialog.
Chapter 4: Connecting From A Web Browser

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 options 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 option 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 55.

Troubleshooting display
If the mouse cursor is not behaving in the expected way, turn off Render cursor locally. If the screen is not updating properly, turn off Fast CopyRect. These options are 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. See Copying and pasting text between client and host computers on page 64 for more information.

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 53. The VNC clipboard dialog opens:

Disabling and enabling copy and paste
You can disable copy and paste while the current connection is in progress. To do this, open the Options dialog. For more information on this dialog, see Using the Options dialog on page 54. On the Inputs tab, turn off Accept clipboard from VNC Server and Send clipboard to VNC Server.

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

This chapter explains how to use VNC Viewer to exchange information with the host computer, or with other VNC Viewer 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 4.6 connectivity* on page 12.

**Contents**

- Printing host computer files to a local printer 58
- Transferring files between client and host computers 60
- Copying and pasting text between client and host computers 64
- Communicating securely using chat 65
Chapter 5: Exchanging Information

Printing host computer files to a local printer

You can print host computer files directly to the default printer attached to your 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 the 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 58.

If the host computer file does not print to the local printer, start with Troubleshooting printing on page 59.

Disabling and enabling printing

You can disable printing providing you do so before you connect. Open the Options dialog and, on the Printing tab, choose Don't share a printer. For more information, see Configuring printing on page 33.

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 will have a name of the form <printer name> via VNC from <client computer name>, for example HP Color LaserJet CP2020 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 options 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.
Chapter 5: Exchanging Information

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 at least version 4.5 of VNC Viewer and VNC Server respectively? Printing is not supported by earlier versions. See also Connecting to a different VNC Server on page 12 for an inter-version incompatibility.

2. Printing is not supported if either client or host computer are running HP-UX, AIX, Solaris 8, or Windows NT 4. In addition, under Solaris 9 and 10, SUSE Linux, and systems with SE Linux enabled, prior configuration is required. For more information, see www.realvnc.com/products/enterprise/4.6/unix.html.

3. 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.

4. VNC Viewer may have been configured to disable printing. To see how to enable it again, read Disabling and enabling printing on page 58. You will have to close the current connection and then reconnect.

5. VNC Viewer may have been configured to prevent the local printer becoming the host computer's default, which means it 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 58. 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, note it will have a name of the form `<printer name>` via VNC from `<client computer name>`, for example HP Color LaserJet CP2020 via VNC from Neptune.

6. 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 89.

7. 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 108.

8. 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 it, 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 89.

9. 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.

The file transfer mechanism described in this section is new to VNC Enterprise Edition 4.6. If you are connecting to a previous version of VNC Server, or from a previous version of VNC Viewer, some steps will be different. Refer to the User Guide for that version, available from the RealVNC web site.

If file transfer fails for any reason, see Troubleshooting file transfer on page 63.

Sending files to a host computer

To send files to a host computer:

1. Click the File Transfer VNC Viewer toolbar button. The File Transfer - VNC Viewer dialog opens on the client computer:

![File Transfer - VNC Viewer dialog]

(Windows XP)

2. Click the Send files button. A Send Files dialog opens.

3. Select a file or folder. To select multiple files and/or folders, hold down the SHIFT key.

   Note: Under Windows, you cannot directly select a folder. Instead, double-click to open that folder, then click Use Entire Folder. To select multiple folders, open the parent folder and click Use Entire Folder. Note this means other files and folders in the parent folder will also be transferred.
4. Click **Open** (OK under UNIX or Linux). The **File Transfer - VNC Server** dialog opens on the host computer:

![File Transfer - VNC Server dialog]

(Ubuntu 10.04 Linux)

The most recent file transfer operation is highlighted. You can check its status, or pause or stop the transfer if it takes more than a few seconds.

By default, files are downloaded to the host computer’s desktop (Downloads folder under Mac OS X). To change this for future file transfer operations, select an option from the **Fetch files to** dropdown at the bottom of the **File Transfer - VNC Server** dialog. Note you must have write permissions for the folder you choose. Alternatively, you can ask to be prompted each time.
Chapter 5: Exchanging Information

Fetching files from a host computer

You can fetch files from a host computer. Note that other VNC Viewer users connected at the same time as you will also receive the files. To do this:

1. In the VNC Viewer window, right-click the VNC Server icon (shaded black) and, from the shortcut menu, select File Transfer. For more information on this icon, and where it can be found, see Using the VNC Server icon on page 77. The File Transfer - VNC Server dialog opens on the host computer:

   ![File Transfer - VNC Server dialog](Ubuntu 10.04 Linux)

2. Click the Send files button. A Send Files dialog opens.

3. Select a file or folder. To select multiple files and/or folders, hold down the SHIFT key.

   Note: Under Windows, you cannot directly select a folder. Instead, double-click to open that folder, then click Use Entire Folder. To select multiple folders, open the parent folder and click Use Entire Folder. Note this means other files and/or folders in the parent folder will also be transferred.
4. Click **Open (OK)** under UNIX or Linux. The **File Transfer - VNC Viewer** dialog opens on the client computer:

![File Transfer - VNC Viewer dialog](Ubuntu 10.04 Linux)

The most recent file transfer operation is highlighted. You can check its status, or pause or stop the transfer if it takes more than a few seconds.

By default, files are downloaded to the client computer's desktop (Downloads folder under Mac OS X). To change this for future file transfer operations, select an option from the **Fetch files to** dropdown at the bottom of the **File Transfer - VNC Viewer** dialog. Note you must have write permissions for the folder you choose. Alternatively, you can ask to be prompted each time.

**Disabling and enabling file transfer**

You can disable file transfer while the current connection is in progress. To do this, open the **Options** dialog and, on the **Inputs** tab, turn off **Enable file transfer**. For more information on this dialog, see *Using the Options dialog* on page 39. The **File Transfer** 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. Are you connecting to **VNC Server** for Windows 4.5 in Service Mode? See *Connecting to a different VNC Server* on page 12 for an inter-version incompatibility.

2. **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 63.

3. **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 89.

4. 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 108.

5. Under UNIX or Linux, for VNC Server in Virtual Mode, a program called vncconfig 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 vncconfig in a Terminal window, and press the ENTER key.

Note that under some versions of UNIX, a VNC Server icon is not 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.)

You can copy and paste text from an application on the host computer to one on the client. Note that text copied can also be pasted by all other users connected at the same time as you. To do this:

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 65.

### Disabling and enabling copy and paste

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

To do this, open the Options dialog and, on the Inputs tab, turn off Share clipboard with VNC Server. For more information on this dialog, see Using the Options dialog on page 39.
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 64.
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 89.
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 108.
4. By default, a maximum of 256kB of text can be copied and pasted. If this number of bytes is exceeded, the entire paste operation fails, and the last text copied to the Clipboard is pasted instead.
5. Under UNIX or Linux, for **VNC Server** in Virtual Mode, a program called `vncconfig` 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 `vncconfig` in a Terminal window, and press the ENTER key.

Note that under some versions of UNIX, a **VNC Server** icon is not available. However, copy and paste may still be enabled in this case.

**Communicating securely using 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 **Chat - VNC Viewer** message box appears at the bottom of the **VNC Viewer** window:

![Chat - VNC Viewer](Windows XP)
Enter a message and click the **Send** button. The message is broadcast to a **Chat - VNC Server** dialog that opens on the host computer, visible to you and to all other connected users (including a host computer user, if present):

![Chat - VNC Server dialog](image)

(Ubuntu 10.04 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.

**Chatting 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 78.

![VNC Server shortcut menu](image)

(Ubuntu 10.04 Linux)

2. Select **Chat**. The **Chat - VNC Server** dialog opens. Type text in the field at the bottom:
3. Press the ENTER key to send the message:

![Chat - VNC Server]

(Ubuntu 10.04 Linux)

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

**Working with chat**

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

![Chat - VNC Viewer]

(Windows XP)

Note that the Chat - VNC Server dialog can also be minimized. If so, you are notified when new messages appear by the taskbar button flashing (Windows and UNIX or Linux) or a number overlaid on the dock icon (Mac OS X).

Chat messages are stored on the host computer for 90 days. To stop recording messages, select Tools > Options in the Chat - VNC Server dialog and turn off Log chat history. Alternatively, you can reduce the number of days, or switch to storing a particular number of messages.

To clear the conversation window, 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 first stop VNC Server, delete the file, and then restart.

Note that when a VNC Viewer user disconnects, messages sent by that user change color in the Chat - VNC Server dialog.
Chapter 5: Exchanging Information

Disabling and enabling chat

You can disable chat while the current connection is in progress.

To do this, open the Options dialog and, on the Inputs tab, turn off Enable chat. For more information on this dialog, see Using the Options dialog on page 39. The Start Chat Session VNC Viewer toolbar button is disabled.

Note: Chat is only disabled for you, and not for any other connected VNC Viewer user. You can still view messages in the Chat - VNC Server dialog.

You can enable chat again at any time.

Troubleshooting chat

If you cannot use chat, check the following:

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

For more information on this dialog, see Using the VNC Server dialog on page 79.

2. VNC Viewer may have been configured to disable chat. To see how to enable it again, read Disabling and enabling chat on page 68.

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 89.

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 108.
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 all 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 host computer user to be present in order for it to work, and should therefore be avoided.

Note: For more information on security, see Chapter 7, Securing Connections on page 91.

Contents

Starting VNC Server 70
Running multiple instances of VNC Server 74
Working with VNC Server 77
Configuring network communications 83
Notifying when users connect 85
Preventing connections to VNC Server 87
Restricting functionality for connected users 88
Stopping VNC Server 90
Chapter 6: Setting Up VNC Server

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 are able to connect. To delay or prevent connections, see Preventing connections to VNC Server on page 87.

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 74.

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 on page 73.

• In User Mode, select RealVNC > Advanced > VNC Server (User Mode) from the Start menu.

Note: Due to Microsoft User Account Control, VNC Server in User Mode severely restricts connected users from fully controlling a host computer running Windows Vista or later.

The VNC Server dialog opens:

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

The VNC Server dialog is the gateway to VNC Server and all its operations. For more information, see Using the VNC Server dialog on page 79.

Click the Close button to minimize the VNC Server 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 77.

To see how to stop VNC Server, or to learn why VNC Server might stop automatically, read Stopping VNC Server on page 90.
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 74.

To start VNC Server:

• In User Mode, either:
  — Type `x0vncserver` in a Terminal window, and press the ENTER key. Note you should not be a user with administrative privileges when you run this command.
  — Select Applications > Internet > VNC Server (User Mode) from the menu system, if available.

The VNC Server dialog opens:

![VNC Server (User-Mode)](image)

(Ubuntu 10.04 Linux)

The VNC Server dialog is the gateway to VNC Server in User Mode and all its operations. For more information, see Using the VNC Server dialog on page 79.

Under most versions of UNIX and Linux, you can click the Close button to minimize the VNC Server 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 77 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. Note you should not be a user with administrative privileges when you run this command. A message ending with text similar to the following appears:

```plaintext
New desktop is johndoe:1 (192.168.2.187:1)
```
Chapter 6: Setting Up VNC Server

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 dialog comparable to those 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 on page 73.

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 83.

To see how to stop VNC Server, or to learn why VNC Server might stop automatically, read Stopping VNC Server on page 90.

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 74.

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.

The VNC Server dialog opens:

(Mac OS X 10.6. In this example, VNC Server is in Service Mode.)

The VNC Server dialog is the gateway to VNC Server and all its operations. For more information, see Using the VNC Server dialog on page 79.
Click the **Close** button to minimize the VNC Server dialog but keep VNC Server running in the background.

To access the dialog again, click the VNC Server icon in the Status bar and, from the shortcut menu, select **Status**. For more information, see Using the VNC Server icon on page 77.

To see how to stop VNC Server, or to learn why VNC Server might stop automatically, read Stopping VNC Server on page 90.

**Preventing VNC Server starting automatically**

*Note:* The information in this section applies to VNC Server for Windows only.

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

To prevent VNC Server in Service Mode starting automatically, open the Options dialog and turn off **Start VNC Server automatically with Windows**. For more information, see Using the Options dialog on page 82.

**Working with VNC Server in Virtual Mode**

*Note:* The information in this section applies to VNC Server for UNIX or Linux only.

VNC Server in Virtual Mode starts unattached to any physical display hardware. This means that desktop artifacts to help you work with VNC Server, such as a VNC Server icon and VNC Server 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.
Chapter 6: Setting Up VNC Server

**Note:** To see how to use VNC Viewer to connect to VNC Server, read *Connecting to a host computer* on page 33. 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 visible to the connected user. For more information on this icon, including how to use it to open the VNC Server dialog and configure VNC Server, start with *Using the VNC Server icon* on page 77.

**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 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 70.

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.

**Note:** VNC Server in User Mode severely restricts connected users from fully controlling host computers running Windows Vista or later. A connected user loses mouse and keyboard control if a program requiring administrative privileges is run (this may or may not be preceded by a User Account Control prompt). The connected user can only continue if a host computer user closes the program, or accepts the prompt.

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 92.

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 83 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 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 92.

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 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 on page 73.
- 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 92.

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 83 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 90.

**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 at log on and 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 92.

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 turned on.) 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 92.

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 83 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](image)

- Under most versions of UNIX or Linux, for VNC Server in User Mode, in the Notification Area:
  ![Ubuntu 8.10 Linux](image)

  **Note:** A VNC Server icon cannot be displayed for VNC Server in User Mode under some versions of UNIX. For VNC Server in Virtual Mode, a VNC Server icon is only available to a connected user; see Working with VNC Server in Virtual Mode on page 73 for more information.

- Under Mac OS X, in the Status bar:
  ![Mac OS X 10.5](image)

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:
  ![VNC Server icon](image)

  Open the VNC Server dialog to begin diagnosing the problem. For more information, see Using the VNC Server dialog on page 79.

- Confirms whether users are connected or not. When the first user connects, the icon is shaded black:
  ![VNC Server icon](image)

  When the last user disconnects, the icon reverts color again.
Chapter 6: Setting Up VNC Server

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

  ![VNC Server Icon](image)

  *(Windows XP)*

- Has a shortcut menu that performs useful operations, such as opening the VNC Server dialog. For more information, see Using the VNC Server shortcut menu on page 78.

  **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 dialog, but cannot normally configure VNC Server. For more information, see Using the VNC Server dialog on page 79.

### 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:

```
<table>
<thead>
<tr>
<th>Option</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Opens the VNC Server dialog. For more information, see Using the VNC Server dialog on page 79.</td>
</tr>
<tr>
<td>Connect to Listening VNC Viewer</td>
<td>Opens the Connect to Listening VNC Viewer dialog. You can establish a reverse connection in conjunction with a client computer user. For more information, see Establishing a reverse connection on page 102.</td>
</tr>
<tr>
<td>Disconnect VNC Viewers</td>
<td>Disconnects all users (including web browser users). Note that, by default, users can immediately reconnect.</td>
</tr>
<tr>
<td>Guest Login</td>
<td>When turned on, and providing VNC Server is configured correctly, a Guest is allowed to connect, bypassing VNC Server’s authentication mechanism. For more information, see Allowing a Guest to connect on page 100.</td>
</tr>
<tr>
<td>Chat</td>
<td>Opens the Chat - VNC Server dialog. You can send messages to all connected VNC Viewer users (not web browser users). For more information, see Communicating securely using chat on page 65.</td>
</tr>
</tbody>
</table>
```

78 VNC Enterprise Edition 4.6 User Guide
Chapter 6: Setting Up VNC Server

Using the VNC Server dialog

The VNC Server dialog is the gateway to VNC Server, and the first port of call for connection information and troubleshooting. It also provides access to the Options dialog, enabling you to configure VNC Server.

Note: A connected user can open the VNC Server dialog but cannot configure VNC Server unless the currently logged on host computer user has administrative privileges. For more information on privileges, see Authenticating connections to VNC Server on page 92.

<table>
<thead>
<tr>
<th>Option</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Transfer</td>
<td>Opens the File Transfer - VNC Server dialog. You can send files and/or folders to all connected VNC Viewer users (not web browser users).</td>
</tr>
<tr>
<td>Stop VNC Server</td>
<td>Stops VNC Server, disconnecting all users (including web browser users). You may be required to confirm this operation. For more information, see Stopping VNC Server on page 90.</td>
</tr>
</tbody>
</table>

(Windows XP)

To open the VNC Server 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, a VNC Server dialog is only visible to a connected user; see Working with VNC Server in Virtual Mode on page 73 for more information.

The title bar of the VNC Server dialog confirms which mode VNC Server is running in. For more information on modes, see Running multiple instances of VNC Server on page 74.
Chapter 6: Setting Up VNC Server

The VNC Server dialog provides access to the Options dialog, enabling you to configure VNC Server. To open it, click the Options button. You may be required to confirm this operation. For more information, start with Using the Options dialog on page 82.

Troubleshooting

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

![VNC Server is working normally in Service Mode](what is this?)

This should mean users can immediately connect.

If an amber warning ⚠️ or red error ❌ is shown instead, click the [details] link to begin diagnosing the problem, for example:

Not accepting connections [details]

Port conflicts are a common source of connection problems. See Configuring network communications on page 83 for more information.

Identifying the host computer

The VNC Server dialog confirms:

- The network address of the host computer, and the port number on which VNC Server is listening for connection requests if not the registered default, 5900:

  ![Address: 192.168.2.133:5901](copy | test | show all | IPv6 info)

  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 within a private network (click the [copy] link to copy this to the Clipboard). Note that users connecting over the Internet must typically enter the network address of the router protecting the host computer instead. To find out what this is, click the [test] link. For more information on these issues, see Step 3: Identify VNC Server and the host computer on page 17.

  Note 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 cannot be used if the [IPv6 info] link is visible; see Preventing connections from particular client computers on page 105 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://192.168.2.133:5900](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 48.

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 83.

Confirming the number of connected users

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

2 users connected

Click the [details] link to manage connected users. The Active Connections dialog opens:

(Windows XP)

In this example, the user present 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, the name could alternatively be Admin or Guest, or be left blank. For more information on authentication, start with Authenticating connections to VNC Server on page 92.

- Has a Full set of VNC permissions, permitting unrestricted access to functionality while the connection is in progress. For more information, see Restricting functionality for particular connected users on page 108.

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

By default, VNC Server displays a notification message in the bottom right corner of the host computer's desktop (top right under Mac OS X) when each user connects and disconnects:

(Windows XP)
You can configure VNC Server so that notification occurs in different ways, or not at all. For more information, start with Notifying when users connect on page 85.

Displaying the VNC Server signature

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

```
VNC Server signature: 2e7ac2a4-003-062-2e67 [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 112.

Warning of trial license expiry

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

```
Trial license installed, 30 days remaining [details]
```

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

Using the Options dialog

The Options dialog enables you to configure VNC Server:

(Windows XP. In this example, the dialog is in Advanced mode.)
To open the Options dialog, click the Options button on the VNC Server dialog. For more information on this dialog, see Using the VNC Server dialog on page 79.

**Note:** Under UNIX or Linux, for VNC Server in Virtual Mode, an Options dialog is only available to a connected user; see Working with VNC Server in Virtual Mode on page 73 for more information.

The first time you open this dialog, it opens in Basic mode, and only one tab is available, containing the most common options. 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 options in this dialog, see the subsequent sections in this chapter, starting with Configuring network communications on page 83. For more information on the options in the Security area of the Connections tab, and security in general, see Chapter 7, Securing Connections on page 91.

Note that configuring an option affects all future connections. Unless otherwise stated in the sections that follow, configuring an option 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 74.

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 85 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.
Chapter 6: Setting Up VNC Server

Port conflicts disable VNC Server. You should be able to resolve them by changing the ports on which VNC Server listens. To do this, change options on the Connections tab of the Options dialog. For more information on this dialog, see Using the Options dialog on page 82.

(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 connect. 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 changing this option 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 download. 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 changing these options 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 options does not affect currently connected users.

**Notifying when users connect**

By default, *VNC Server* displays a notification message in the bottom right corner of the host computer’s desktop (top right under Mac OS X) each time a *VNC Viewer* or web browser user connects:

| (Windows XP) |

**Note:** A similar message appears on disconnection.
You can choose different notification options on the **Connections** tab of the **Options** dialog. For more information on this dialog, see *Using the Options dialog* on page 82.

![Options dialog](image)

*(Windows XP)*

**Preventing notification messages**

You can disable notification messages for both connection and disconnection. To do this, choose **Do nothing**.

**Displaying connection prompts**

You can replace notification messages with connection prompts that enable a host computer user (or an already-connected user) to identify newly-connecting users and accept or reject them. To do this, choose **Show accept/reject prompt**.

**Note:** Some connecting users (those with sufficient VNC permissions) are able to bypass connection prompts.

Alternatively, you can *conditionally* replace notification messages with connection prompts so that they only appear when a host computer user is ‘present’ to accept or reject them. To do this, choose **Show prompt if user logged on** *(VNC Server in Service Mode)* or **Show prompt if user connected** *(VNC Server in Virtual Mode)*. For information on the distinction, and on connection prompts in general, see *Preventing particular users connecting* on page 107.
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 a host computer.

You can prevent all users connecting by configuring options on the Connections tab of the Options dialog. For more information on this dialog, see Using the Options dialog on page 82.

Note: You can prevent particular users connecting, or connections from particular client computers; see Preventing particular connections to VNC Server on page 105 for more information.

(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 option does not affect currently connected users.

Note: If the Options dialog is in Basic mode, this 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 102.

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 option 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 options on the Inputs tab of the Options dialog. For more information on this dialog, see Using the Options dialog on page 82.

(Windows XP)

**Note:** You can restrict access to VNC Enterprise Edition functionality for particular users by revoking VNC permissions; see Restricting functionality for particular connected users on page 108 for more information.
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 must 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 all client computer mice. 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 option is on the Printing tab. For more information about this feature, see Printing host computer files to a local printer on page 58.

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 60.

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 64.

Note: Under Windows, note that files can be copied and pasted by VNC Viewer users to client computers also running Windows. To prevent this, turn off Share files with VNC Viewers.

Preventing chat

You can prevent VNC Viewer users communicating securely using chat. To do this, turn off Enable chat. For more information about this feature, see Communicating securely using chat on page 65.
Chapter 6: Setting Up VNC Server

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 71.
- 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 77.

Note that VNC Server automatically stops:

- In User Mode (all platforms), when the host computer starting it logs off 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 on page 73.
- 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 option is changed to Logoff user. For more information, see Protecting the host computer on page 114.
- A connected user logged on as a host computer user with administrative privileges can explicitly stop VNC Server.
- A connected user can log off and/or power the host computer off.

To see how to start VNC Server again, read Starting VNC Server on page 70.
Securing Connections

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. Conversely, you can tighten the encryption rules if necessary.

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 from connecting at all.

Contents

Authenticating connections to VNC Server 92
Relaxing the authentication rules 97
Bypassing the authentication rules 100
Changing the encryption rules 103
Preventing particular connections to VNC Server 105
Restricting functionality for particular connected users 108
Uniquely identifying VNC Server 112
Protecting privacy 113
Chapter 7: Securing Connections

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 97.

By default, under all platforms, VNC Server specifies system authentication. This means that a connecting user must supply the credentials (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: System 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 a password set on the primary user account (this might be the case with friends and family, for example). If so, the default authentication mechanism must be changed to either VNC password or None. A connecting user cannot specify a blank password in order to connect.

Windows

Under Windows, system authentication is specified by the default Windows password option in the Authentication dropdown of the Options dialog. For more information on this dialog, see Using the Options dialog on page 82.

(Windows XP)
Chapter 7: Securing Connections

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 96.

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 108.

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, system authentication is specified by the default UNIX password option in the Authentication dropdown of the Options dialog. For more information on this dialog, see Using the Options dialog on page 82.

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 96.

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 108.

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, system authentication is specified by the default Mac password option in the Authentication dropdown of the Options dialog. For more information on this dialog, see Using the Options dialog on page 82.

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 96.

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 108.

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 to Mac OS X 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 system 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 system 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 97.)

To manage users and groups in the authentication list, open the Options dialog. For more information on this dialog, see Using the Options dialog on page 82. On the Connections tab, click the Configure button. Providing either Windows password (or platform-specific equivalent) or Single sign-on (where available) 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:** Artifacts in this dialog have slightly different names under UNIX or Linux and Mac OS X.

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 connecting users supplying those credentials, 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 108.

### Relaxing the authentication rules

By default, VNC Server specifies system 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 92.

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', forgo the need to distribute host computer user credentials, or enable older versions of VNC Viewer (or VNC-compatible Viewer technology) that do not support authentication to connect. Note that some mechanisms allocate VNC permissions in ways that cannot be customized.

To change the authentication mechanism, open the Options dialog. For more information on this dialog, see Using the Options dialog on page 82. On the Connections tab, select an alternative to Windows password (or platform-specific equivalent) from the Authentication dropdown:

(Windows XP)
Chapter 7: Securing Connections

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

**Single sign on**

The **single sign-on** authentication mechanism extends system authentication to automatically authenticate a connecting user to any instance of VNC Server on any host computer using the credentials initially supplied 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 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 system authentication, and can be customized. For more information, see the appropriate platform-specific section in Authenticating connections to VNC Server on page 92.

**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 in this dialog, 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 an admin 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 view only password.

When connecting to VNC Server, a user sees the VNC Viewer Authentication Credentials dialog:

![Authentication Credentials 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 admin password in the Password field, a Full set of VNC permissions is granted.

- ViewOnly in the Username field, and the view only 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 108. 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, or in order to enable older versions of VNC Viewer, or VNC-compatible Viewer technology, to connect. Note you can allow just particular users to connect without supplying a password; see Bypassing the authentication rules on page 100 for more information.

**Note:** The None option is only available in the Authentication dropdown when the Options dialog is in Advanced mode. For more information, see Using the Options dialog on page 82.

A Default set of VNC permissions is granted to each connected user. For more information, see Restricting functionality for particular connected users on page 108. 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.

To do this, you can either:

- 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 102 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 either of 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 97.

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 allow a Guest, open the Options dialog. For more information on this dialog, see Using the Options dialog on page 82. On the Connections tab, select an alternative to the default None option from the Guest access dropdown:

(Windows XP)
To grant 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 108. Note you cannot customize VNC permissions for Guests.

To enable a Guest to connect, a host computer user must also 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 78. A tick appears:

(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 sees the VNC Viewer Authentication Credentials dialog:

(Windows XP)

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

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

(Windows XP)
Chapter 7: Securing Connections

A host computer user must accept 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 107.

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.

Note this feature is also 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 standard 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 78.

   (Windows XP)

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

   (Windows XP)

3. If you are connecting:
   - Within a private network, enter the network address of the client computer itself. If you do not know this, you can ask a client computer user to run a command such as `ipconfig` (Windows) or `ifconfig` (Linux and Mac OS X).
— Over the Internet, enter the network address of a router protecting the client computer. If you do not know this, you can ask a client computer user to visit www.whatismyip.com.

For more information on private and public networks, start with Connecting within a private network on page 21.

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 on 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 can control the host computer exactly as 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 108. Note you cannot customize VNC permissions for Listening VNC Viewer users.

Changing the encryption rules

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

Note: A connecting user can request that the encryption rules be tightened, but not relaxed.

You can configure VNC Server to:

• 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, or VNC-compatible Viewer technology, that do not support encryption to connect. For more information on eavesdropping, see Uniquely identifying VNC Server on page 112.

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

• Tighten the encryption rules by increasing the AES key size to 256-bit. This makes connections ultra-secure, but may impact performance. It also means only VNC Viewer 4.6 or later can connect.
Chapter 7: Securing Connections

To change the rules, open the Options dialog. For more information on this dialog, see Using the Options dialog on page 82. On the Connections tab, select an alternative to the default Always on option from the Encryption dropdown:

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

**Always maximum**

Encryption is always on. The AES key size is always 256-bit. Choose this option to ensure only VNC Viewer 4.6 or later can connect.

A connecting user cannot request that encryption be turned off, or the AES key size reduced to 128-bit.

**Prefer on**

Encryption is preferably on. A connecting user can request either that it be turned off (by selecting Prefer off in the VNC Viewer dialog), or that the AES key size be increased to 256-bit (by selecting Always maximum in the VNC Viewer dialog).

**Prefer off**

Encryption is preferably off. Choose this option to allow older versions of VNC Viewer, or VNC-compatible Viewer technology, to connect.

A connecting user can request that encryption be turned back on, either to 128-bit AES (by selecting Prefer on or Always on in the VNC Viewer dialog), or 256-bit AES (by selecting Always maximum in the VNC Viewer dialog).

For more information about requesting encryption in the VNC Viewer dialog, see Step 4: Request an encryption option on page 19.
Preventing particular connections to VNC Server

You can prevent particular users connecting to VNC Server. 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 107 for more information.

**Note:** You can prevent all users connecting to VNC Server. For more information, see Preventing connections to VNC Server on page 87.

Preventing connections from particular client computers

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

**Note:** If you filter network addresses, users can no longer enter host computer IPv6 network addresses in order to connect to VNC Server (even from an authorized client computer).

To filter network addresses, open the **Options** dialog. For more information on this dialog, see Using the Options dialog on page 82. On the **Connections** tab, click the **IP Filter** button. The **IP Address Filter Rules** dialog opens:

![IP Address Filter Rules](Windows XP)

(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 Add Rule dialog opens:

(Windows XP)

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept the connection</td>
<td>Accepts connection requests from the specified client computer(s).</td>
</tr>
<tr>
<td>Reject the connection</td>
<td>Rejects connection requests from the specified client computer(s).</td>
</tr>
<tr>
<td>Ask the VNC Server user what to do</td>
<td>Displays connection prompts enabling a host computer user either to accept connection requests, allow 'view only' access, or reject requests from the specified client computer(s). If no host computer user is present, connection requests are automatically rejected after 10 seconds. For more information on connection prompts, see Preventing particular users connecting on page 107.</td>
</tr>
</tbody>
</table>

Note that if you filter network addresses, the order of rules in the IP Address Filter Rules 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 are always rejected. You can move rules up and down in the dialog using the 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. Note this rule is always last 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:

A connection prompt enables a host computer user (if one is present), or an already-connected user, to identify the connecting user and either accept the connection request, allow ‘view only’ access to the host computer, or reject the request. If no response is received within ten seconds, then the connection request is automatically rejected. Note that 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 connecting user supplying credentials that grant a Full set of VNC permissions is able to bypass connection prompts. Such a user cannot be prevented connecting. You can configure VNC permissions to either permit more users to bypass connection prompts, or to submit all users to them. For more information, see Customizing VNC permissions on page 109.

To display connection prompts, open the Options dialog. For more information on this dialog, see Using the Options dialog on page 82. On the Connections tab, choose Show accept/reject prompt from the When VNC Viewers connect dropdown:
In certain circumstances, you may be able to conditionally display connection prompts:

- For VNC Server in Service Mode (Windows and Mac OS X), choose Show prompt if user logged on in order to automatically accept connections when no host computer user is currently logged on (and therefore unlikely to be present). Note that at least one newly-connected user must then log on to the operating system of the host computer in order to continue. Subsequently, connection prompts are displayed again, for this user to accept or reject.

- For VNC Server in Virtual Mode (UNIX or Linux), choose Show prompt if user connected to automatically accept the first connection (since no host computer user can be ‘present’ at a virtual desktop). Subsequently, connection prompts are displayed again, for this user to accept or reject.

For more information on notifications, see Notifying when users connect on page 85.

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:

<table>
<thead>
<tr>
<th>VNC Server authentication mechanism</th>
<th>Credentials supplied in order to connect</th>
<th>Set of VNC permissions granted</th>
<th>Customizable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>System authentication or Single sign-on</td>
<td>Host computer user with administrative privileges</td>
<td>Full</td>
<td>YES</td>
</tr>
<tr>
<td>VNC password</td>
<td>Any other host computer user</td>
<td>Default</td>
<td>YES</td>
</tr>
<tr>
<td>VNC password</td>
<td>Generic password (no user name)</td>
<td>Default</td>
<td>NO</td>
</tr>
<tr>
<td>VNC password</td>
<td>Admin user name and admin password</td>
<td>Full</td>
<td>NO</td>
</tr>
<tr>
<td>VNC password</td>
<td>ViewOnly user name and view only password</td>
<td>View Only</td>
<td>NO</td>
</tr>
</tbody>
</table>

For information on system authentication, see Authenticating connections to VNC Server on page 92. For information on the other authentication mechanisms, see Relaxing the authentication rules on page 97.

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

<table>
<thead>
<tr>
<th>Type of user</th>
<th>Credentials supplied in order to connect</th>
<th>Set of VNC permissions granted</th>
<th>Customizable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest (Interactive)</td>
<td>Guest user name (no password)</td>
<td>Default</td>
<td>NO</td>
</tr>
<tr>
<td>Guest (View-only)</td>
<td></td>
<td>View Only</td>
<td>NO</td>
</tr>
</tbody>
</table>

108 VNC Enterprise Edition 4.6 User Guide
Chapter 7: Securing Connections

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

<table>
<thead>
<tr>
<th>Permission name</th>
<th>When granted, a connected user can...</th>
<th>Full</th>
<th>Default</th>
<th>View Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>View display contents</td>
<td>See the host computer's desktop.</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Send pointer events</td>
<td>Control the host computer using the client computer's mouse.</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Send keyboard events</td>
<td>Control the host computer using the client computer's keyboard.</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Send and receive clipboard contents</td>
<td>Copy and paste text between applications running on the client and host computers.</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Send and receive files</td>
<td>Exchange files with the host computer.</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Add VNC printers</td>
<td>Print host computer files to a local printer.</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Accept chat messages</td>
<td>Chat with other VNC Viewer users, or with a host computer user.</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Connect without accept/reject prompt</td>
<td>Bypass connection prompts. For more information about this feature, see Preventing particular users connecting on page 107.</td>
<td>YES</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Customizing VNC permissions

If VNC Server specifies system 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 if VNC Server specifies any other authentication mechanism, or for users who bypass authentication.

Note: You can restrict access to VNC Enterprise Edition functionality for all connected users by configuring options on the Inputs tab of the Options dialog. For more information, see Restricting functionality for connected users on page 88.

To customize VNC permissions, open the Options dialog. For more information on this dialog, see Using the Options dialog on page 82. On the Connections tab, click the Configure button. Providing either

For more information on these types of user, see Bypassing the authentication rules on page 100.
Windows password (or platform-specific equivalent) or Single sign-on (where available) 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 96.

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. The connected user cannot copy and paste or bypass connection prompts and, if a VNC Viewer user, cannot print, chat, or transfer files.
Chapter 7: Securing Connections

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.

The VNC Server signature is displayed in the VNC Server dialog:

![VNC Server (User-Mode) dialog](image)

(Ubuntu 10.04)

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:

![VNC Viewer](image)

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:

```
*** WARNING: The VNC Server's signature has changed since you last connected to it. ***

Unless there is a good reason for the signature to have changed, you should not continue connecting.

The new VNC Server signature is 37-bd-62-3b-76-69-12-1d.

Do you wish to accept the new signature and continue connecting?
```

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.

### Protecting privacy

**Note:** The information in this section applies to VNC Server for 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, and if a host computer user is present, then that user can observe the operations of connected users.

Under Windows, you can configure VNC Server to uphold the privacy of connected users by editing various options in the Options dialog. For more information on this dialog, see Using the Options dialog on page 82.

**Note:** A connecting user may be able to ensure their own privacy by disconnecting all other users when they connect. For more information, see Disconnecting other users 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 option 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 option 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. 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.

  For VNC Server in Service Mode, users can immediately reconnect, but must know how to unlock the host computer in order to continue. For VNC Server in User Mode, users can immediately reconnect, but see only a non-operational black screen, and cannot continue.

• Logging off, select Logoff user.

  For VNC Server in Service Mode, users can immediately reconnect, but must know how to log on to the host computer in order to continue. For VNC Server in User Mode, users cannot connect, since VNC Server stops. See Stopping VNC Server on page 90 for more information.
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 only, 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.

If you are using either 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 modes, see VNC Enterprise Edition 4.6 connectivity on page 12.

Contents

Saving connections to VNC Address Book 116
Using VNC Address Book to connect 121
Managing connections using VNC Address Book 122
Saving connections to desktop icons 125
Appendix A: Saving Connections

Saving connections to VNC Address Book

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

Connecting from VNC Address Book means you do not have to remember a network address and port number for VNC Server, nor a user name and password. In addition, VNC Address Book automatically recreates the VNC Viewer environment you choose for controlling that host computer the first time, for example the scaling applied to the desktop, the encryption level, 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, see Working with the master password on page 124.

You can use VNC Address Book to organize connections, configure the appearance and behavior of VNC Viewer for particular connections, 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 at any time. To do this:

1. Click the Save Connection VNC Viewer toolbar button. VNC Address Book opens. 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** in order to forget the password. You will need to enter it each time you connect from 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 also 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 edit the connection). Note that a protected connection is identified by a padlock symbol throughout VNC Address Book.
2. 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:

![Enter Master Password dialog box](image)

*(Windows XP)*

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

![VNC Address Book](image)

*(Windows XP)*

To see how to use *VNC Address Book* to connect to this host computer again in future, read *Using VNC Address Book to connect* on page 121.

For more information on editing and organizing connections, start with *Organizing connections* on page 123.
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 122. The VNC Address Book dialog opens:
2. Click the **New Entry** toolbar button. The **Properties** dialog opens:

![Properties dialog](image)

(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 and 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 edit 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 edit VNC Viewer options in order to set up your preferred environment for controlling this host computer. To do this, use the **Basic** tab to configure common options, 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:

```
Enter Master Password
```

(Windows XP)

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

```
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 121.

For more information on editing and organizing connections, start with Organizing connections on page 123.
Using VNC Address Book to connect

You can use VNC Address Book to quickly connect to a host computer:

1. Start VNC Address Book on the client computer. To see how to do this, read Starting VNC Address Book on page 122. The VNC Address Book dialog opens:

   (Windows XP)

   2. Either:

   — Double-click a connection in the Alphabetic or Hierarchical list.

   — Select a connection in a 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 124.

   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 122.
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 Tools > 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:

![VNC Address Book icon](image)

**Note:** Under UNIX or Linux and Mac OS X, no VNC Address Book icon is available. However, most 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:

![Quick Launch Bar](image)

To open the quick launch bar, click the VNC Address Book icon.
• Has a right-click shortcut menu that performs useful operations:

<table>
<thead>
<tr>
<th>Shortcut menu option</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect to</td>
<td>Opens a menu where you can select a host computer to connect to.</td>
</tr>
<tr>
<td>Launch VNC Viewer</td>
<td>Starts VNC Viewer, enabling you to connect to a new host computer in the standard way. For more information, see Connecting to a host computer on page 33.</td>
</tr>
<tr>
<td>Open Address Book</td>
<td>Opens the VNC Address Book dialog, enabling you to create new connections or edit and organize existing ones. (Alternatively, double-click the VNC Address Book icon.)</td>
</tr>
<tr>
<td>Exit</td>
<td>Closes VNC Address Book.</td>
</tr>
</tbody>
</table>

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

Organizing connections

VNC Address Book organizes connections both alphabetically and hierarchically:

You can reorganize connections in the Hierarchical list. (The Alphabetical list is automatically organized.)

Click the New Folder toolbar button to create folders in the Hierarchical 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 be required to enter the VNC Address Book master password first.

To do this, select a connection in the Alphabetical or Hierarchical list, and either:
Appendix A: Saving Connections

- Click the Properties tool button.
- Select Edit > Properties.

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

To rename a connection in VNC Address Book, select it in the Alphabetical or Hierarchical 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 Alphabetical or Hierarchical 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 list, and either:
- Click the Delete tool 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 editing the connection.

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 116.
By default, VNC Address Book remembers the master password for one hour. This means you have 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. Click the **Save Connection** VNC Viewer toolbar button.
   **Note:** For fully-featured VNC Viewer, you must first disable **VNC Address Book**. To do this, click the **Options** VNC Viewer toolbar button to open the **Options** dialog and, on the **Expert** tab, set the **UseAddrBook** parameter 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.