

VNC® User Guide

Version 5.3

December 2015

Trademarks

RealVNC, VNC and RFB are trademarks of RealVNC Limited and are protected by trademark registrations and/or pending trademark applications in the European Union, United States of America and other jurisdictions. Other trademarks are the property of their respective owners.

Protected by UK patent 2481870; US patent 8760366

Copyright

Copyright © RealVNC Limited, 2002-2015. 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

Contents

	About This Guide	7
Chapter 1:	Introduction	9
	Principles of VNC remote control	10
	Getting two computers ready to use	11
	Connectivity and feature matrix	13
	What to read next	17
Chapter 2:	Getting Connected	19
	Step 1: Ensure VNC Server is running on the host computer	20
	Step 2: Start VNC Viewer on the client computer	21
	Step 3: Identify VNC Server running on the host computer	21
	Step 4: Request an encrypted connection	22
	Step 5: Connect to VNC Server	23
	Troubleshooting connection	26
Chapter 3:	Using VNC Viewer	35
	Starting VNC Viewer	36
	Starting Listening VNC Viewer	36
	Configuring VNC Viewer before you connect	37
	Connecting to a host computer	39
	The VNC Viewer user experience	40
	Using the toolbar	42
	Using the shortcut menu	43
	Using the Options dialog	44
	Managing the current connection	45
	Changing appearance and behavior	46
	Restricting access to features	48

Chapter 4:	Connecting From A Web Browser	51
	Connecting to a host computer	52
	The VNC Viewer for Java user experience	56
	Working with VNC Viewer for Java	57
Chapter 5:	Exchanging Information	61
	Printing host computer files to a local printer	62
	Transferring files between client and host computers	64
	Copying and pasting text between client and host computers	68
	Communicating securely using chat	69
Chapter 6:	Working With VNC Server	73
	Licensing VNC Server	74
	Starting VNC Server	75
	Running VNC Server	78
	Keeping VNC Server up-to-date	81
	The VNC Server user interface	82
	Troubleshooting VNC Server	87
	Configuring VNC Server	89
	Changing ports	90
	Notifying when users connect	92
	Stopping VNC Server	93
Chapter 7:	Making Connections Secure	95
	Authenticating users	96
	Authenticating using system credentials	96
	Authenticating using a password specific to VNC	98
	Relaxing the authentication rules	100
	Bypassing the authentication rules	102
	Changing the encryption rules	105
	Preventing connections to VNC Server	106
	Restricting functionality for connected users	110

	Verifying the identity of VNC Server	115
	Protecting privacy	116
Appendix A:	Saving Connections	117
	Saving connections to VNC Address Book	118
	Using VNC Address Book to connect	123
	Managing connections using VNC Address Book	124
	Saving connections to desktop icons	127
Appendix B:	Setting Up VNC	129
	Configuring VNC	130
	Specifying VNC parameters	130
	Specifying Xvnc options	136
	Preventing users configuring VNC	138
	Managing system authentication	141
	Setting up single sign-on authentication	142
	Hosting VNC on a UNIX network share	144
	Logging information	147
	Completely removing VNC	149

About This Guide

This Guide explains how to use *VNC 5.x* remote access and control software from RealVNC to connect two computers over a network, and control one from the other.

Applicable software

All the information in this Guide applies to connections established between a client computer running the latest version of *VNC Viewer* and a host computer running the same version of *VNC Server* with an Enterprise license. Unless otherwise stated, this combination is assumed. To see how to set these applications up, read *Getting two computers ready to use* on page 11.

Note that general principles of remote control, and information relating to particular supported features, also applies to connections established between any combination of the products and license types listed below.

VNC Server (with different license types applied)

- *VNC Server* with a Personal license
Contains most VNC remote control features. A thirty day trial is available.
- *VNC Server* with a Free license
Contains basic remote control features.

For more information on licensing, start with *Licensing VNC Server* on page 74.

VNC Viewer

- *VNC Viewer for Java*
This application is freely available to download on demand from *VNC Server* with an Enterprise or a Personal license.
- *VNC Viewer Plus*
This application is available to purchase from www.realvnc.com/products/viewerplus/.
- *VNC Viewer for iOS*
This application is freely available from the Apple App Store. Visit www.realvnc.com/products/ios/ for more information.
- *VNC Viewer for Android*
This application is freely available from Google Play. Visit www.realvnc.com/products/android/ for more information.
- *VNC Viewer for Google Chrome*
This application is freely available from the Google Chrome Web Store. Visit www.realvnc.com/products/chrome/ for more information.

To understand restrictions for connections established between particular combinations of products and license types, see *Connectivity and feature matrix* on page 13.

Intended audience

There is no such thing as a typical RealVNC user or remote control session. This Guide therefore has more than one audience in mind:

- Chapter 1 is a general introduction to remote control, 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 remote computer to be controlled.
- Appendices B, C, and D are intended for system administrators responsible for deploying, licensing, and configuring VNC 5.x in an enterprise environment.

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

Conventions

Screen captures are from Windows 7 unless otherwise stated. Dialogs and other artifacts may appear differently under UNIX and Mac OS X, or versions of Windows with different themes, but the principle is the same.

Contacting Technical Support

You can contact Technical Support if you have an Enterprise or a Personal license to use *VNC Server* and your support and upgrades contract is valid. This contract lasts for a minimum of one year from the date of purchase of the license, and can be renewed. To see whether it is valid, examine the **Details** section of the **VNC Server** dialog, or run the command `vnclicense -list`.

To obtain support, visit support.realvnc.com. For information about critical security patches and product upgrades, see *Keeping VNC Server up-to-date on page 81*.

Related information

Visit www.realvnc.com for:

- Supported platforms, operating systems, and system requirements.
- Instructions on how to install and uninstall VNC 5.x.
- Release notes, Knowledge Base articles, forums, and FAQs.
- Information relating to legacy *VNC Enterprise Edition* and *VNC Personal Edition*.
- Information relating to other RealVNC products and solutions.

Introduction

This Guide explains how to use *VNC 5.x* remote access and control software from RealVNC to connect two computers over a network and take control of one (the *host computer*) from the other (a *client computer*), irrespective of where the two are in the world, or incompatibilities they may have in platform, architecture, or operating system.

VNC 5.x consists of two components: *VNC Server* and *VNC Viewer*. All the information in this Guide applies to connections established between a client computer running the latest version of *VNC Viewer* and a host computer running the same version of *VNC Server* with an Enterprise license. For a list of other products and license types to which information may also apply, see *Applicable software on page 7*.

Contents

Principles of VNC remote control	10
Getting two computers ready to use	11
Connectivity and feature matrix	13
What to read next	17

Principles of VNC remote control

To connect to and control one computer from another:

- An application called *VNC Server* must be running on the host computer; that is, on the computer you want to control. To see how to obtain, license, and start *VNC Server*, read *Setting up the host computer* on page 11.

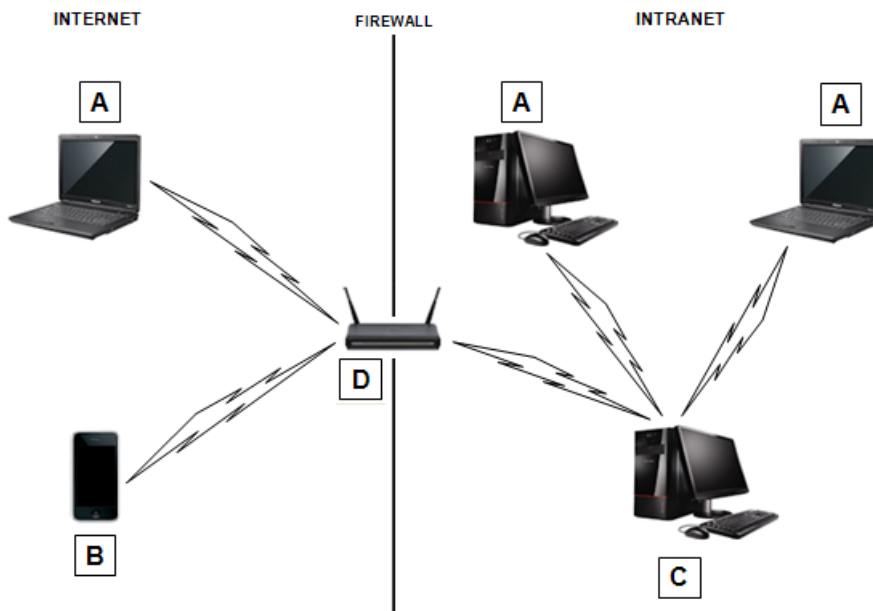
Note: You may be able to control computers that are running alternatives to *VNC Server*. For more information, see *Connecting to VNC-compatible Server software* on page 15.

- An application called *VNC Viewer* must be running on the client computer; that is, on the computer you are sitting in front of, and want to exercise control from. To see how to obtain and start *VNC Viewer*, read *Setting up the client computer* on page 12.

Note: You may be able to exercise control using alternatives to *VNC Viewer*. For more information, see *Connecting from alternatives to VNC Viewer* on page 15.

- Host and client computers must be connected to the same TCP/IP network. This can be a private network such as a LAN or VPN, or a public network such as the Internet. Note that firewalls and routers must typically be configured before an Internet connection can be established. See *Connecting over the Internet* on page 28 for more information.

Consider the following example:



A. Client computer (typically a laptop or desktop) running VNC Viewer. **B.** Client device (handset or tablet) running VNC Viewer for iOS or Android. **C.** Host computer (typically a workstation or server) running VNC Server. **D.** Router exposing a public network address for Internet connections to the host computer.

To start a remote control session, run *VNC Viewer* and identify *VNC Server* on the host computer you want to control. Once authenticated, *VNC Viewer* displays the host computer's desktop in a new window, and you can take control using the client computer's keyboard and mouse (or device touch). 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. *See a picture.*

Note: By default, *VNC Server* allows other users to connect to the host computer at the same time as you. You may be sharing control.

VNC 5.x remote access and control software solves different problems for users with different requirements, from the family member troubleshooting computer problems over the Internet to the system administrator configuring devices remotely in an enterprise environment. To find out how to get the information you need from this Guide, see *What to read next* on page 17.

Getting two computers ready to use

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

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.

Setting up the 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. This can be:
 - 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 (4G/3G/GPRS/EDGE).
2. Download and install *VNC 5.x* from www.realvnc.com/download/vnc/, and license *VNC Server* (note administrative privileges are required). For more information on licensing, start with *Licensing VNC Server* on page 74.
3. If you are connecting over a public network such as the Internet, it is very likely that 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 31 for more information.
4. If you are connecting over a public network such as the Internet, it is very likely that 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 29.

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 20 for more information.
6. Find out the network address of *VNC Server*. If you are connecting:
 - Over a LAN or VPN, this is a private address, which is that of the host computer itself. See *Connecting within a private network* on page 28 for more information.
 - Over the Internet, this is a public address, which is that of a router or similar device acting as a public gateway. See *Connecting over the Internet* on page 28 for more information.
7. Find out the credentials required to authenticate to *VNC Server*. By default, if you are connecting to:
 - *VNC Server* with an Enterprise or a Personal license, you require the user name and password of a user account with administrative privileges on the host computer. See *Authenticating using system credentials* on page 96 for more information.
 - *VNC Server* with a Free license, you require a password specific to VNC. See *Authenticating using a password specific to VNC* on page 98 for more information.

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

Setting up the 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 (for example, the Internet).
2. Obtain *VNC Viewer*. You can either:
 - Download *VNC Viewer* as a standalone application from www.realvnc.com/download/viewer/, and save the file to an appropriate location. (Depending on the download package chosen, you may need to extract it first.) Under UNIX and Linux, you must also make the file executable, for example by running the command:

```
chmod +x <VNC Viewer download file>
```


Under Mac OS X, you must mount the disk image, for example by double-clicking it, or alternatively by running the command:

```
hdiutil attach <VNC Viewer download file>
```
 - Install *VNC 5.x* from www.realvnc.com/download/vnc/, which incorporates *VNC Viewer*, and for which you do not require a license key. If you do this, *VNC Viewer* can be started from the menu system of most operating systems, which may be more convenient, and in addition you can save connections to *VNC Address Book*. However, note that administrative privileges are typically required to install software.
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 38.

Connectivity and feature matrix

You can use the latest version of *VNC Viewer* to connect to:

- The latest version of *VNC Server* incorporated in *VNC 5.x*.
- Previous versions of *VNC Server* incorporated in *VNC Enterprise Edition* or *VNC Personal Edition*.
- VNC-compatible Server software from third parties.

Note that the latter two may require configuration before a connection can be established, and that not all VNC remote control features will be available once connected.

Note: For alternatives to *VNC Viewer*, see *Connecting from alternatives to VNC Viewer* on page 15.

Connecting to VNC 5.x

You can establish a connection from *VNC Viewer* to the latest version of *VNC Server* incorporated in *VNC 5.x* providing the following conditions are met.

	VNC Server		
	Enterprise	Personal	Free
VNC Viewer	No configuration required.	On the client computer, <i>VNC Viewer</i> encryption must not be set to Always Maximum.	On the client computer, <i>VNC Viewer</i> encryption must not be set to Always Maximum or Always on.

Note: For information on *VNC Viewer* encryption, see *Step 4: Request an encrypted connection* on page 22.

Restrictions

- Connections to *VNC Server* with a Personal license cannot be encrypted using ultra-secure 256-bit AES.
- Connections to *VNC Server* with a Free license cannot be encrypted at all.
- The credentials you enter to log on to your *client* computer cannot authenticate you automatically to *VNC Server* with a Personal license.
- The credentials of a user account on the host computer cannot be used to authenticate to *VNC Server* with a Free license.
- Connections to *VNC Server* with a Free license are not optimized for performance.
- *VNC Viewer for Java* cannot be downloaded from *VNC Server* with a Free license.

Note that once a connection to *VNC Server* with a Free license is established, you cannot perform the following operations:

- Exchange files with the host computer.
- Print host computer files to a local printer.
- Chat with other connected users, or with a host computer user.

Connecting to VNC Enterprise Edition or VNC Personal Edition 4.6

You can establish a connection from *VNC Viewer* to *VNC Server* incorporated in *VNC Enterprise Edition* or *VNC Personal Edition* 4.6 without configuration.

Restrictions

The credentials of a user account on the host computer cannot be used to authenticate to *VNC Personal Edition*.

Connecting to VNC Enterprise Edition or VNC Personal Edition 4.5 or earlier

You can establish a connection from *VNC Viewer* to *VNC Server* incorporated in *VNC Enterprise Edition* or *VNC Personal Edition* 4.5 or earlier providing the following conditions are met.

	VNC Server	
	VNC Enterprise Edition 4.5-	VNC Personal Edition 4.5-
VNC Viewer	On the client computer, <i>VNC Viewer</i> encryption must not be set to Always Maximum.	On the client computer, <i>VNC Viewer</i> encryption must not be set to Always Maximum.

Restrictions

- Connections to *VNC Enterprise Edition* and *VNC Personal Edition* cannot be encrypted using ultra-secure 256-bit AES.
- The credentials of a user account on the host computer cannot be used to authenticate to *VNC Personal Edition*.

Once a connection is established, you cannot:

- Exchange files with *VNC Enterprise Edition* or *VNC Personal Edition* 4.3 or earlier. Note under Windows, there are also certain restrictions when connected to version 4.5 and 4.4 as well.
- Print *VNC Enterprise Edition* or *VNC Personal Edition* 4.4 or earlier files.
- Chat with *VNC Enterprise Edition* or *VNC Personal Edition* 4.4 or earlier users.

Connecting to VNC-compatible Server software

You can establish a connection from *VNC Viewer* to the following (selected) third party VNC-compatible Server software providing certain conditions are met.

	VNC-Compatible Server software		
	Apple Remote Desktop or Screen Sharing built-in to Mac OS X	Remote Desktop or Desktop Sharing built-in to Ubuntu	Community projects such as TightVNC or UltraVNC
VNC Viewer	<p>On the host computer, VNC viewers may control screen with password must be turned on, and a password set.</p> <p>On the client computer, <i>VNC Viewer</i> encryption must not be set to Always Maximum or Always on.</p>	<p>On the host computer, Allow other users to view your desktop and Allow other users to control your desktop must be turned on.</p> <p>On the client computer, <i>VNC Viewer</i> encryption must not be set to Always Maximum or Always on.</p>	<p>On the client computer, <i>VNC Viewer</i> encryption must not be set to Always Maximum or Always on.</p>

Restrictions

Note that only a very limited set of VNC remote control features is available for connections to host computers running VNC-compatible Server software. In particular, connections cannot be encrypted.

Connecting from alternatives to VNC Viewer

You can connect to the latest version of *VNC Server* from the following alternatives to *VNC Viewer*:

- *VNC Viewer for Java*. See *Connecting from VNC Viewer for Java* on page 15.
- *VNC Viewer Plus*. See *Connecting from VNC Viewer Plus* on page 16.
- *VNC Viewer for iOS*. See *Connecting from mobile devices* on page 16.
- *VNC Viewer for Android*. See *Connecting from mobile devices* on page 16.
- *VNC Viewer for Google Chrome*. See *Connecting from VNC Viewer for Google Chrome* on page 16.
- VNC-compatible Viewer software from third parties. See *Connecting from VNC-compatible Viewer software* on page 17.

Connecting from VNC Viewer for Java

You can use any modern web browser to download *VNC Viewer for Java* on demand from *VNC Server* with an Enterprise or a Personal license, and then immediately connect.

Note: You cannot download *VNC Viewer for Java* from *VNC Server* with a Free license.

You do not require administrative privileges in order to download and use *VNC Viewer for Java*. For more information, see *Chapter 4, Connecting From A Web Browser* on page 51.

Restrictions

Once a connection is established, you cannot:

- Exchange files with the host computer.
- Print host computer files.
- Chat with other connected users, or with a host computer user.
- Save connections.
- Scale the host computer's desktop.

Connecting from VNC Viewer Plus

You can purchase and install *VNC Viewer Plus* from www.realvnc.com/products/viewerplus/.

In order to make a standard VNC connection, select **VNC** from the **Connection Mode** dropdown on the **VNC Viewer Plus** dialog.

Restrictions

Once a connection is established, you cannot save connections to *VNC Address Book*.

Connecting from mobile devices

You can download and install:

- *VNC Viewer for iOS* from the Apple App Store. Visit www.realvnc.com/products/ios/ for more information.
- *VNC Viewer for Android* from Google Play. Visit www.realvnc.com/products/android/ for more information.

Restrictions

Once a connection is established, you cannot:

- Exchange files with the host computer.
- Print host computer files.
- Make the connection view only.
- Chat with other connected users, or with a host computer user.

Connecting from VNC Viewer for Google Chrome

If you have the Google Chrome web browser version 25 or later, you can download and install *VNC Viewer for Google Chrome* from the Google Chrome Web Store for free, and use it to connect.

You do not require administrative privileges in order to download and use *VNC Viewer for Google Chrome*. For more information, visit www.realvnc.com/products/chrome/.

Restrictions

Once a connection is established, you cannot:

- Exchange files with the host computer.
- Print host computer files.

- Copy and paste text
- Chat with other connected users, or with a host computer user.
- Save connections.
- Scale the host computer's desktop.

Connecting from VNC-compatible Viewer software

Other organizations offer VNC-compatible Viewer applications, for example Remote Desktop Viewer built-in to Ubuntu.

If you wish to allow connections to *VNC Server* with an Enterprise or a Personal license, make sure:

- Encryption is turned off. See *Changing the encryption rules on page 105*.
- System authentication or single sign-on are not selected. See *Relaxing the authentication rules on page 100*.

Restrictions

Note that *no* VNC remote control features are available for connections from client computers running VNC-compatible Viewer software. In particular, connections cannot be encrypted.

What to read next

RealVNC remote control software can be used in many different ways to solve many different kinds of problem. There is no such thing as a typical RealVNC user or remote control session.

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 the 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.

RealVNC remote control software 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 User Guide are targeted at more experienced users, likely to require the power of changing options – system administrators setting up *VNC Server* 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 19.
- 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 35.
- 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 51.
- To see how to exchange information between client and host computers, read *Chapter 5, Exchanging Information* on page 61.

Chapter 1: Introduction

- To learn how to configure *VNC Server* on the host computer, and for advanced topics such as running of *VNC Server*, see *Chapter 6, Working With VNC Server on page 73*.
- By default, *VNC Server* authenticates connecting users and, depending on the license, encrypts connections end-to-end. To learn more about security, and how to relax the rules if you consider it safe to do so, read *Chapter 7, Making Connections Secure on page 95*.

2

Getting Connected

This chapter aims to help the majority of users get started establishing their first connection from a client computer running the latest version of *VNC Viewer* to a host computer running the same version of *VNC Server* with an Enterprise license. For a list of other products and license types to which these instructions may also apply, see *Applicable software on page 7*.

Note: This chapter assumes both host and client computers are set up correctly. For more information, see *Getting two computers ready to use on page 11*.

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 Technical Support. Alternatively, if you are connecting within a private network such as a corporate Local Area Network (LAN), consult your system administrator.

Contents

Step 1: Ensure VNC Server is running on the host computer	20
Step 2: Start VNC Viewer on the client computer	21
Step 3: Identify VNC Server running on the host computer	21
Step 4: Request an encrypted connection	22
Step 5: Connect to VNC Server	23
Troubleshooting connection	26

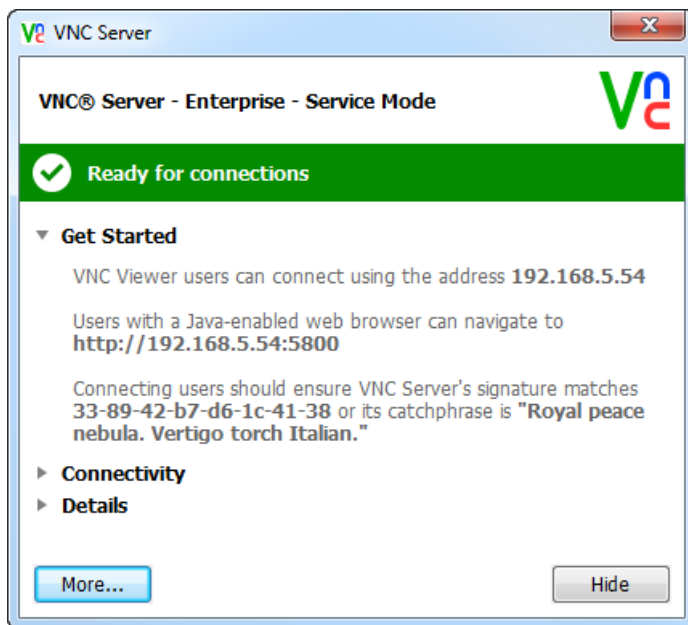
Step 1: Ensure VNC Server is running on the host computer

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, search for or navigate to the **VNC Server** program, or double-click the *VNC Server* shortcut icon, if available on the desktop. Note administrative privileges are required.
- Under UNIX, search for or navigate to the **VNC Server (User Mode)** program.
- Under Mac OS X, search for or navigate to the **VNC Server** program. Note administrative privileges are required.

Note: For alternatives ways to start *VNC Server*, and more information about different modes, see *Starting VNC Server on page 75*.

The **VNC Server** dialog opens:



If the status bar is green, *VNC Server* should be licensed and configured correctly for connections.

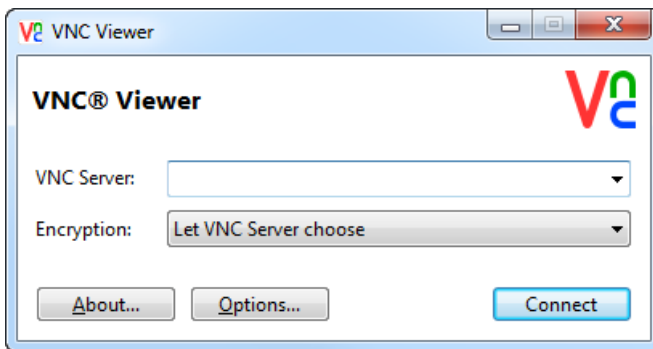
If *VNC Server* is not licensed, or it is not configured correctly, the status bar turns red. Click the **Show** button that appears, and follow the instructions. For more information, consult *Troubleshooting connection on page 26*.

Step 2: Start VNC Viewer on the client computer

To start *VNC Viewer*, either:

- Double-click the *VNC Viewer* shortcut icon, if available on the desktop.
- Search for or navigate to the **VNC Viewer** program, if *VNC Viewer* is installed on the client computer. See *Setting up the client computer* on page 12 for more information.
- Run the appropriate platform-specific command in a Terminal window or Command Prompt (visit www.realvnc.com/products/vnc/documentation/latest/reference/vncviewer-operations.html).

The **VNC Viewer** dialog opens:



Step 3: Identify VNC Server running on the host computer

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

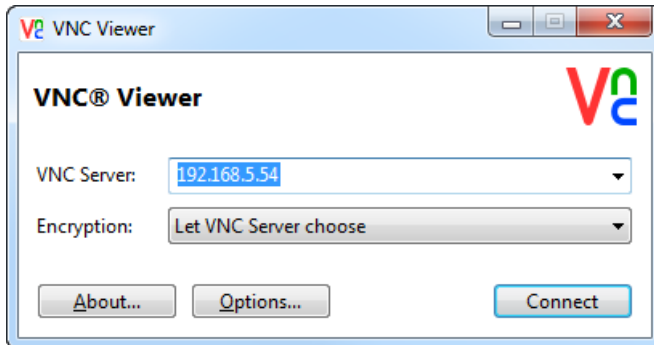
If you are connecting within a private network such as a LAN or VPN, enter the network address of the host computer itself in the **VNC Server** dropdown. This address can take the following forms:

- A host name, for example `john.doe`. (Note the host computer may not have a host name.)
- An IP address in IPv4 format, for example `192.168.5.54`.
- An IP address in IPv6 format within square brackets, for example `[2001:db8::1]`. (Note IPv6 may not be enabled.)

If you do not know the network address of the host computer, start with *Connecting within a private network* on page 28.

If you are connecting over the Internet, 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 28.

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



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 encrypted connection* on page 22.

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 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:

Connection refused (10061)

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 30.

Step 4: Request an encrypted connection

You can request that the connection be encrypted.

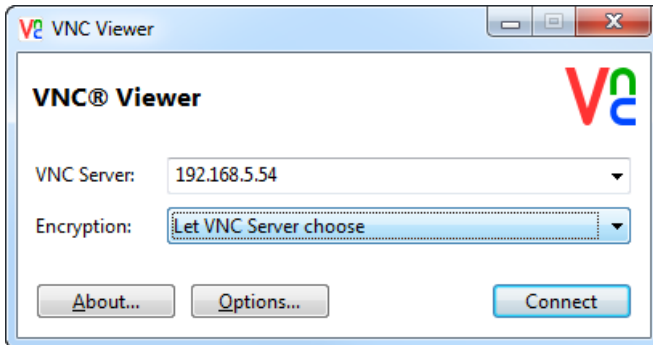
Encryption ensures that data exchanged between the two computers while the connection is in progress cannot be intercepted by third parties. Note that requesting encryption is not a guarantee; *VNC Server* determines whether or not the connection will actually be encrypted.

Note: For more information on encryption, and security in general, see *Chapter 7, Making Connections Secure* on page 95.

By default, connections to *VNC Server* with:

- An Enterprise license are encrypted using industry-standard 128-bit AES. You can request that this be enhanced to ultra-secure 256-bit AES.
- A Personal license are encrypted using industry-standard 128-bit AES.
- A Free license cannot be encrypted. Upgrade to an Enterprise or a Personal license if security is important to you.

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

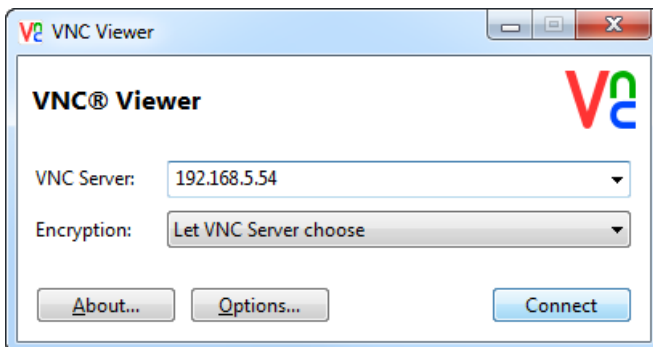


If you are connecting to *VNC Server* with:

- An Enterprise or a Personal license, it is recommended you retain this option unless you have a good reason to either request that encryption be:
 - Enhanced to 256-bit AES for connections to *VNC Server* with an Enterprise license only.
 - Turned off.
 For more information on these operations, see *Changing the encryption rules on page 105*.
- A Free license, do not change this option. Doing so may prevent you connecting. For more information, see *Connectivity and feature matrix on page 13*.

Step 5: Connect to VNC Server

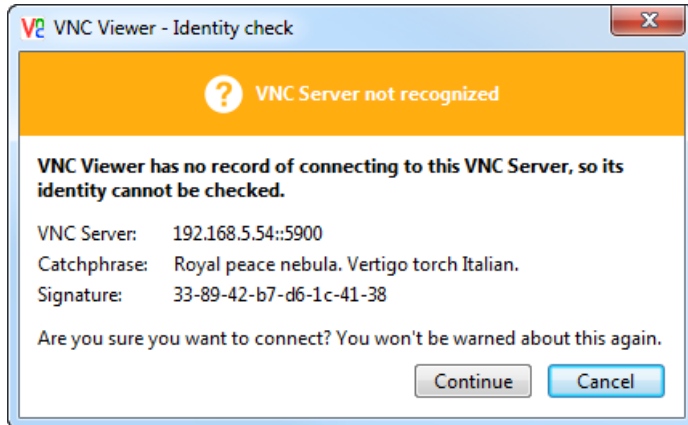
To connect to *VNC Server*, click the **Connect** button at the bottom of the **VNC Viewer** dialog:



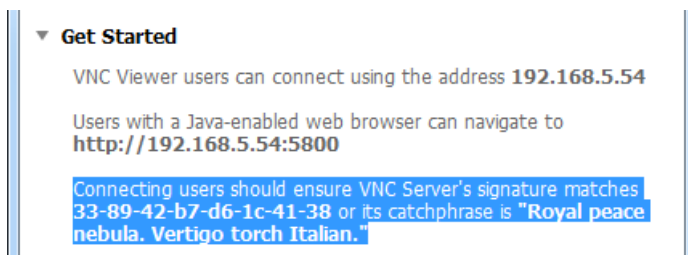
You are guided through steps to ensure that the connection is legitimate and secure.

Checking the identity of VNC Server

If you are connecting to *VNC Server* with an Enterprise or a Personal license, you may see a message similar to the following:



If you have access to the host computer, or can communicate with a host computer user, you can check that *VNC Viewer* is connecting to the intended destination (and not, for example, a malicious third party) by comparing the signature (or more-memorable catchphrase) with that displayed in the **Get Started** section of the **VNC Server** dialog:

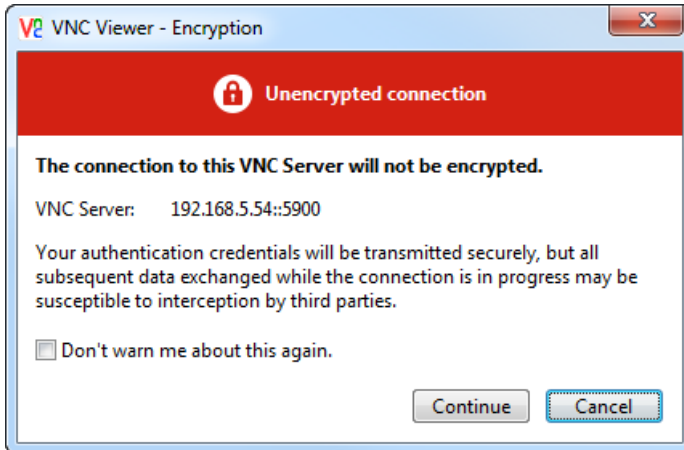


If you see any other message referring to the *VNC Server* signature, it is recommended that you do *not* connect. For more information on this security feature, see *Verifying the identity of VNC Server* on page 115.

Click the **Yes** button to continue connecting to *VNC Server*.

Acknowledging the encryption status

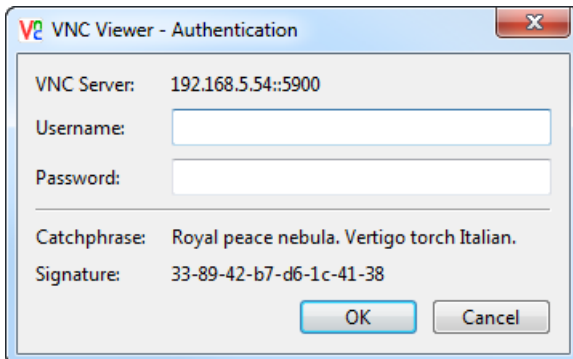
If the connection will not be encrypted, you are prompted to acknowledge that sensitive information may not be secure:



If you are connecting to VNC Server with an Enterprise or a Personal license, you may be able to turn encryption on. Click the **Cancel** button and see *Changing the encryption rules on page 105* for more information. Otherwise, click **Continue**.

Entering authentication credentials

You may be required to enter a user name and/or a password:



By default, if you are connecting to VNC Server with:

- An Enterprise or a Personal license, enter the user name and password you use to *log on* to the host computer. If these system credentials do not work and you have access to the host computer, you may be able to register your user account; see *Authenticating using system credentials on page 96* for more information. If you do not have access, contact a system administrator or a host computer user.
- A Free license, enter the VNC password, leaving the **Username** field blank. If you do not know this password but have access to the host computer, you may be able to reset it; see *Authenticating using a*

password specific to VNC on page 98 for more information. If you do not have access, contact a system administrator or a host computer user.

Click the **OK** button. If the connection succeeds, *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 40*.

If the connection fails for any reason, start with *Troubleshooting connection on page 26*.

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

Troubleshooting connection

This section provides additional information to help you connect. If, after reading this, you still cannot connect:

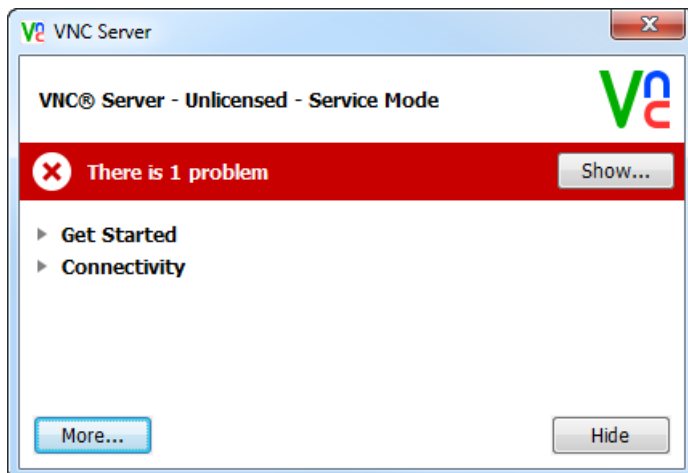
1. Consult www.realvnc.com.
2. You may be eligible to contact Technical Support. Start with *Contacting Technical Support on page 8*.
3. If all else fails, and providing you have a secure network environment and a host computer user is present, you can ask that person to connect to *you*. For more information, see *Establishing a reverse connection on page 102*.

Licensing VNC Server

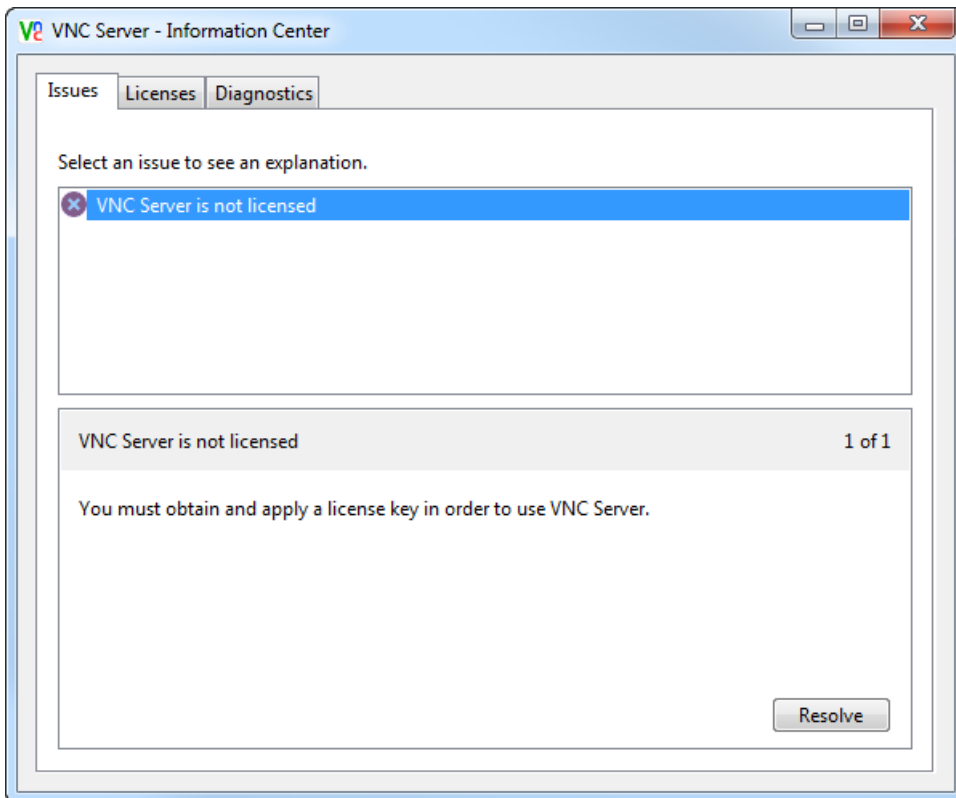
VNC Server must be licensed. If it is not, users cannot connect.

Note: *VNC Viewer* does not require a license key.

If *VNC Server* is not licensed, the status bar on the **VNC Server** dialog turns red:



Click the **Show** button to see more information:

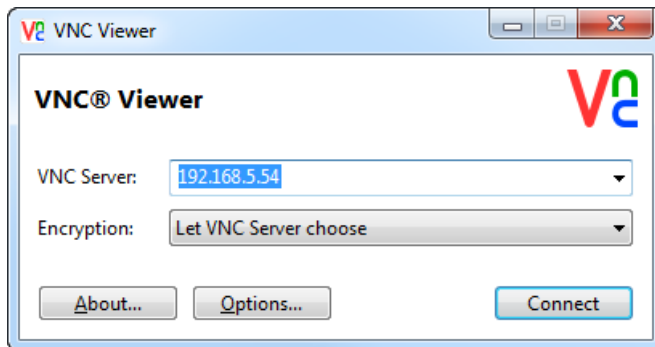


Click the **Resolve** button to start the process of licensing *VNC Server*, and follow the instructions. See *Licensing VNC Server on page 74* for more information.

Connecting within a private network

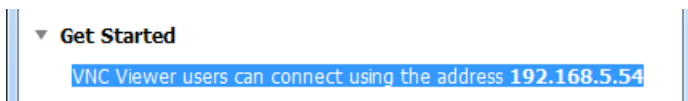
If both client and host computers are managed within a closed network environment such as a LAN or VPN, you are connecting within a *private network*. This is common in corporate and other enterprise environments, and may also be the case if you are connecting two computers at home.

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



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:
 - a. Open the **VNC Server** dialog. *More on this dialog.*
 - b. Examine the appropriate section of the **Get Started** section:

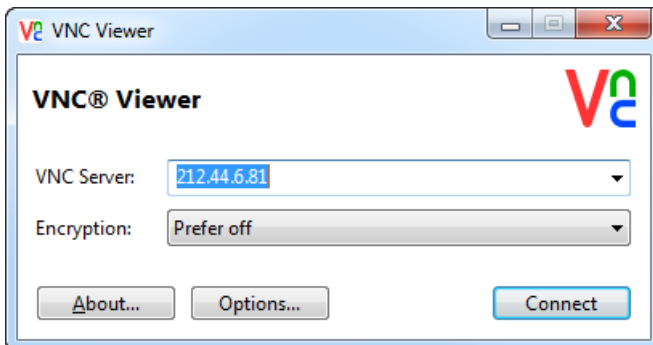


Connecting over the Internet

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.

Note: The host computer is also very likely to be protected by a firewall. For more information, see *Allowing network communications through a firewall* on page 31.

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



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 to visit www.whatismyip.com.
- And you *do* have access to the host computer:
 - a. Open the **VNC Server** shortcut menu. *More on this menu.*
 - b. Choose **Information Center** and, on the **Diagnostics** tab, click the **Test Internet Connection** button.
 - c. 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:

VNC Server appears to be behind a NAT router with IP address 212.44.6.81. You will need to configure that router to forward port 5900 to this computer before you can connect to VNC Server over the Internet.

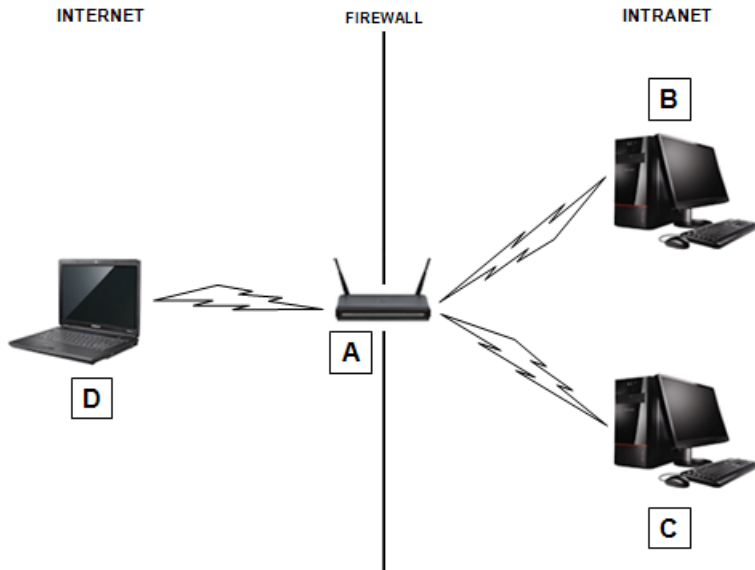
Configuring a router to forward network communications

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.** Client computer running VNC Viewer.

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.

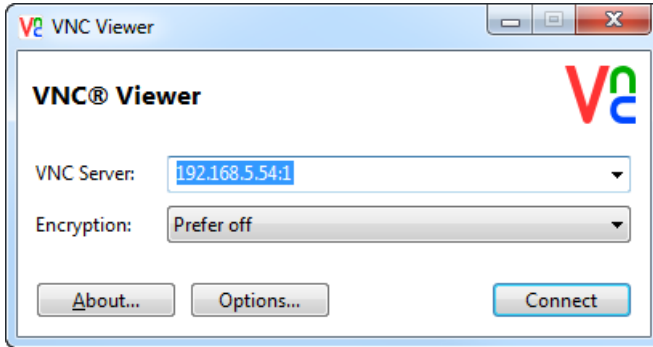
When you connect to either host computer from *VNC Viewer*, you must enter the network address of the router: 212.44.6.81. In addition, to connect to host computer C, you must qualify the router's network address with the port number: 212.44.6.81:1. To find out why this is, see *Qualifying a network address with a port number* on page 30.

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 *Changing ports* on page 90.

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:



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

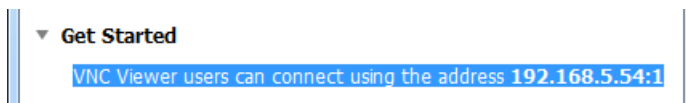
```
johndoe:1
192.168.5.54:1
[2001:db8::1]:1
```

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

```
johndoe::6001
192.168.5.54::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:
 - a. Open the **VNC Server** dialog. *See how to do this.*
 - b. Examine the appropriate section of the **Get Started** section:



In this example, *VNC Server* is running on host computer 192.168.5.54 and listening on port 5901.

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 30.

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*:

```
Connection timed out (10060)
```

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:

```
Either the username was not recognized, or the password was incorrect.
```

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

If you do not know the correct credentials, 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 100*.

Failing to authenticate as 'you'

If you see the following error message:

```
Access is denied.
```

then *VNC Server* has been configured to require the system credentials of a user account on the host computer. *Your* user account, however, has not been registered with *VNC Server*.

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 user account. For more information, see *Managing the list of registered user accounts and groups on page 97*.

Connecting from an unauthorized computer

If you see the following error message:

```
The connection closed unexpectedly.
```

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 107*.

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

Being rejected by a host computer user

If you see the following error message:

```
Connection rejected by host computer user.
```

then *VNC Server* has been configured to display connection prompts, 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-one was present to respond).

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 connection prompts. For more information, see *Preventing particular users connecting on page 109*.

Using VNC Viewer

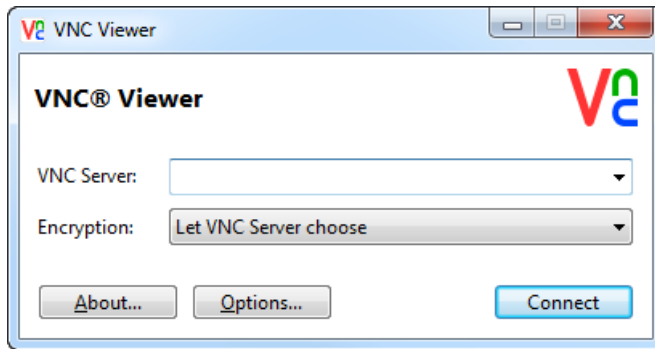
This chapter explains how to control a host computer to which you are connected using *VNC Viewer*, and how *VNC Viewer* features can enhance your productivity while the connection is in progress.

Contents

Starting VNC Viewer	36
Starting Listening VNC Viewer	36
Configuring VNC Viewer before you connect	37
Connecting to a host computer	39
The VNC Viewer user experience	40
Using the toolbar	42
Using the shortcut menu	43
Using the Options dialog	44
Managing the current connection	45
Changing appearance and behavior	46
Restricting access to features	48

Starting VNC Viewer

To start *VNC Viewer*, follow the instructions in *Step 2: Start VNC Viewer on the client computer on page 21*. The **VNC Viewer** dialog appears:



In most circumstances, *VNC Viewer* is ready to connect to *VNC Server* out-of-the-box. Carry on from *Connecting to a host computer on page 39*.

In some circumstances, you may need to configure *VNC Viewer* before you connect. For more information, see *Configuring VNC Viewer before you connect on page 37*.

To see how to start *VNC Viewer* so that it listens for a reverse connection, see *Starting Listening VNC Viewer on page 36*.

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*.

Note: Reverse connections are not secure and should only be used in a locked-down environment.

To start *Listening VNC Viewer*:

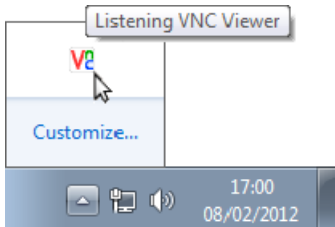
- Under Windows or Mac OS X, search for or navigate to the **Listening VNC Viewer** program.
- Under UNIX, you must start *Listening VNC Viewer* at the command line; visit www.realvnc.com/products/vnc/documentation/latest/reference/vncviewer-operations.html for more information.

Using Listening VNC Viewer

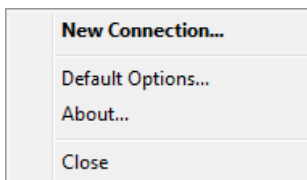
Under Windows and Mac OS X, a *VNC Viewer* icon  is displayed in the Notification area or Status bar respectively when *Listening VNC Viewer* starts. Note that under Windows 7, the Notification area is hidden by default and accessible only from  to the right of the Taskbar.

Note: Under UNIX, no user interface is available for you to work with *Listening VNC Viewer*. If you need to configure it before it starts, read *Specifying VNC parameters on page 130*.

Under Windows and Mac OS X, hover the mouse cursor over the icon to confirm that *Listening VNC Viewer* is running:



The VNC Viewer icon has a shortcut menu:



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 37.

Note: Select **New Connection** to establish a connection to VNC Server in the normal way. Carry on from *Connecting to a host computer* on page 39.

If when a host computer user attempts to establish a reverse connection:

- it is successful, *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 40.
- It is not successful, read *Establishing a reverse connection on page 102* in conjunction with the host computer user.

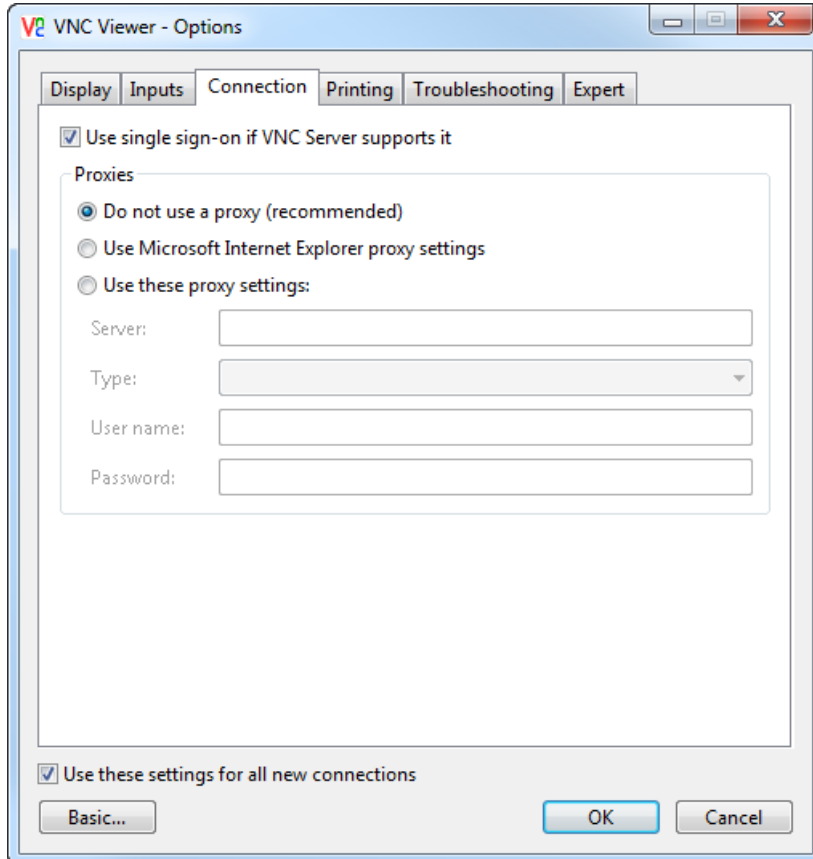
Configuring VNC Viewer before you connect

In most circumstances, *VNC Viewer* is ready to connect to *VNC Server* out-of-the-box. You do not need to configure it. Carry on from *Connecting to a host computer* on page 39.

However, you may need to configure *VNC Viewer* before you connect in the following circumstances:

- Your client computer is protected by a proxy server. See *Connecting via a proxy server* on page 38.
- *VNC Server* mandates the single sign-on authentication scheme but you do not want to authenticate automatically as the user you logged on to the *client* computer as. See *Disabling single sign-on* on page 39.
- You want to specify printing options. See *Configuring printing* on page 39.

To configure *VNC Viewer* before you connect, click the **Options** button at the bottom of the **VNC Viewer** dialog. The **Options** dialog opens:



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

Note that the **Connection** and **Printing** tabs are not available after you connect. *More on this dialog.*

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 you use Internet Explorer and it has already been provisioned with proxy server information. Note this option has a different name under UNIX and Mac OS X, and refers to system proxy environment variables.
- **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.

If the proxy server is protected by BASIC or DIGEST authentication, enter a user name and password in the appropriate boxes.

Disabling single sign-on

Note: The information in this section applies to connections to *VNC Server* with an Enterprise license only.

By default, if *VNC Server* specifies single sign-on as its authentication scheme, then you may be able to connect without supplying a user name and password. This is because you have already successfully authenticated to the system by logging on to your *client* computer. For more information, see *Authenticating users automatically* on page 100.

You can disable this feature if you want to authenticate to *VNC Server* using the credentials of a different user account. This might give you access to a different set of remote control features while the connection is in progress. To do this, turn off **Use single sign-on if VNC Server supports it** on the **Connection** tab.

Configuring printing

By default, when you connect to *VNC Server* with an Enterprise or a Personal license, your 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 your local printer. For more information about this feature, see *Printing host computer files to a local printer* on page 62.

You can print but choose not to change the host computer's default printer. This means you will have to explicitly select your local 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 19.

1. Start *VNC Viewer* on the client computer. The **VNC Viewer** dialog opens.
2. In the **VNC Server** dropdown, enter a private or a public network address for the host computer, qualified, if applicable, by the port number on which *VNC Server* is listening, for example `192.168.5.54:1`.
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 *VNC Server* signature, acknowledge the encryption status, and authenticate to *VNC Server*.

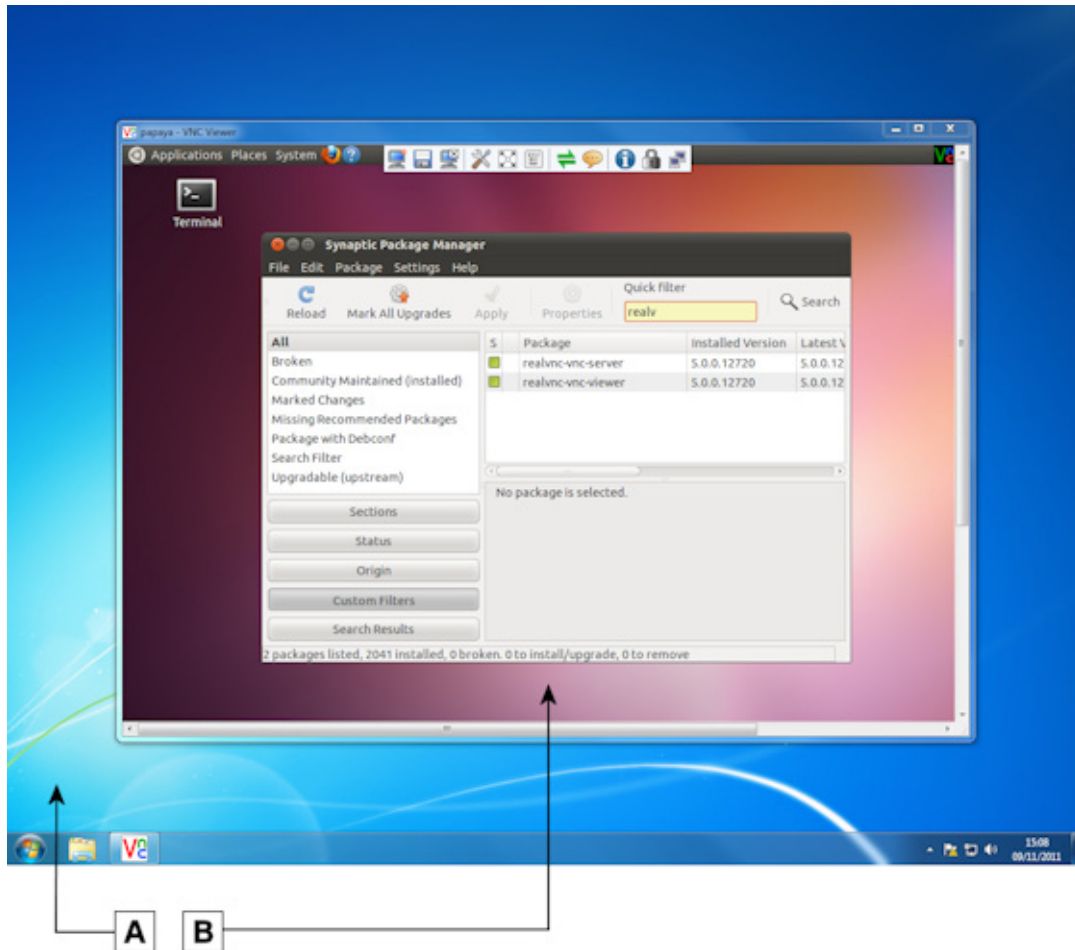
If the connection is successful, *VNC Viewer* displays the host computer's desktop in a new window on the client computer. Carry on from *The VNC Viewer user experience* on page 40. If the connection fails for any reason, start with *Troubleshooting connection* on page 26.

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

The VNC Viewer user experience

The rest of this chapter assumes you are successfully connected to a host computer. If not, see *Connecting to a host computer* on page 39.

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 7. **B.** VNC Viewer displaying the desktop of a host computer running Ubuntu 11.04 Linux.

Note: If the host computer is running UNIX, 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 VNC Server* on page 78.

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 features* on page 48.

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 47 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.

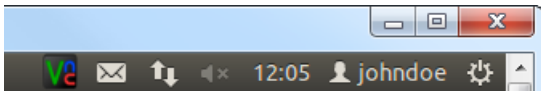
These commands are interpreted by the client computer. Alternative ways of sending them to the host computer are available; start with *Using the shortcut menu* on page 43 for more information. Under Windows and Mac OS X, note you can cause certain other keys and key combinations to be interpreted by your client computer rather than the host. See *Configuring your keyboard* on page 47 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 features* on page 48.

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*; visit www.realvnc.com/products/vnc/documentation/latest/misc/keyboard-mapping/.

Interacting with VNC Server

When you connect, a *VNC Server* icon  and **VNC Server** dialog will likely be available:



(*VNC Server* icon shaded black to indicate a connection is in progress.)

See *The VNC Server user interface* on page 82 for more information.

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 46.

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:



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

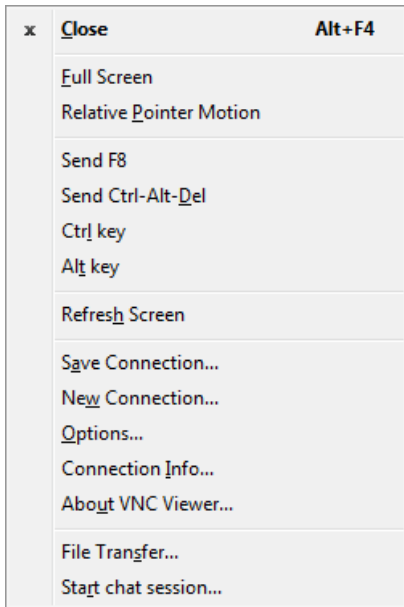
	Button	Purpose
	New Connection	Establish a new connection. See <i>Connecting to a host computer</i> on page 39.
	Save Connection	Save the current connection so you can quickly reconnect without having to remember the network address and authentication credentials. See <i>Appendix A, Saving Connections</i> on page 117.
	Close Connection	Close the current connection (and the VNC Viewer window).
	Options	Configure most aspects of VNC Viewer while the current connection is in progress. See <i>Using the Options dialog</i> on page 44. Note that some options must be configured before you connect. See <i>Configuring VNC Viewer before you connect</i> on page 37.
	Full Screen Mode	Toggle full screen mode on and off.
	Send Ctrl-Alt-Del	Send the CTRL-ALT-DELETE command to the host computer. (Pressing this key combination will be interpreted by the client computer.) You could alternatively press SHIFT-CTRL-ALT-DELETE.
	File Transfer	Browse to the location of client computer files to send to the host computer. See <i>Transferring files between client and host computers</i> on page 64.
	Start Chat Session	Chat with other VNC Viewer users connected to the same host computer, or with a host computer user. See <i>Communicating securely using chat</i> on page 69.
	Connection Information	Display technical information about the current connection, such as the encryption method and compression format. You may need this if you contact Technical Support.
	connection speed	Hover over to reveal the current connection speed. For more information on performance, see <i>Changing appearance and behavior</i> on page 46.

Using the shortcut menu

VNC Viewer has a shortcut menu that facilitates many of the same common operations as the VNC Viewer toolbar. *More on this toolbar.*

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 46.

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):



(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.

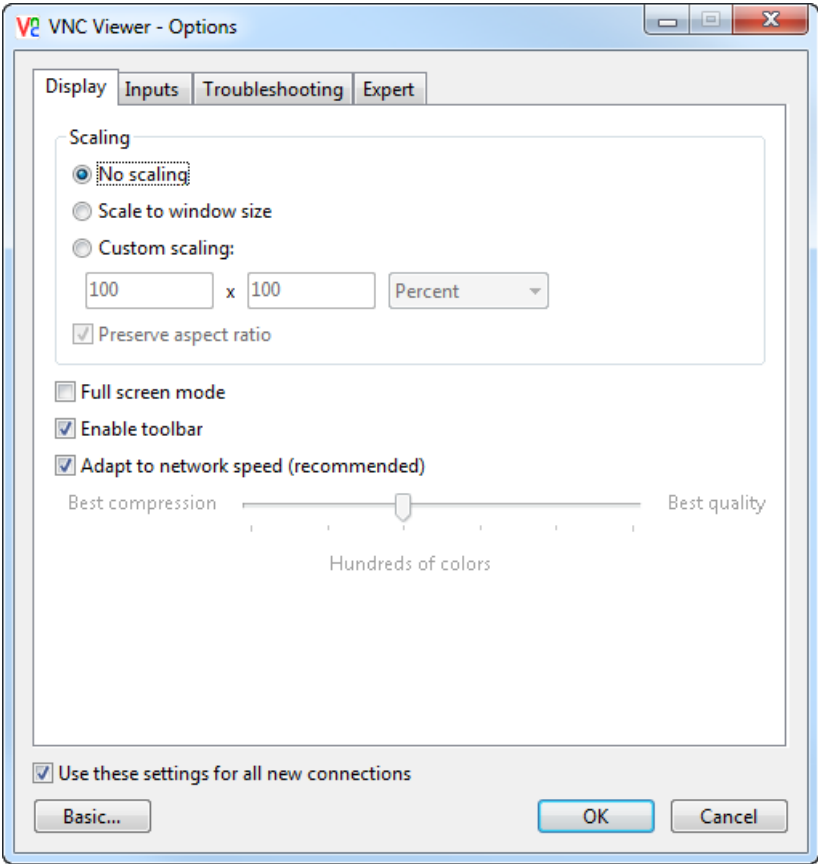
The following table explains the effect of selecting shortcut menu options that do not have equivalent toolbar buttons.

Option	Purpose
Relative Pointer Motion	Turn on if the host computer's mouse cursor appears to be behaving abnormally, for example by accelerating too fast.
Send F8	Send an F8 command to the host computer. (By default, F8 opens the shortcut menu; see <i>Changing the shortcut menu key</i> on page 48 for how to choose a different key.)
Ctrl key	Turn on to simulate holding down the CTRL key.
Alt key	Turn on to simulate holding down the ALT key.
Refresh Screen	Refresh the display of the host computer's desktop.

Option	Purpose
About VNC Viewer	Display version information. You may need this if you contact Technical Support.

Using the Options dialog

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



(In this picture, 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 37.

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 46.)

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.

Many of the options in this dialog are explained in the remainder of this chapter.

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. *More on this toolbar.*


Saving the current connection

You can save the current connection so you can quickly reconnect 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 117.


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 39.

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. *More on this dialog.*

Closing the current connection

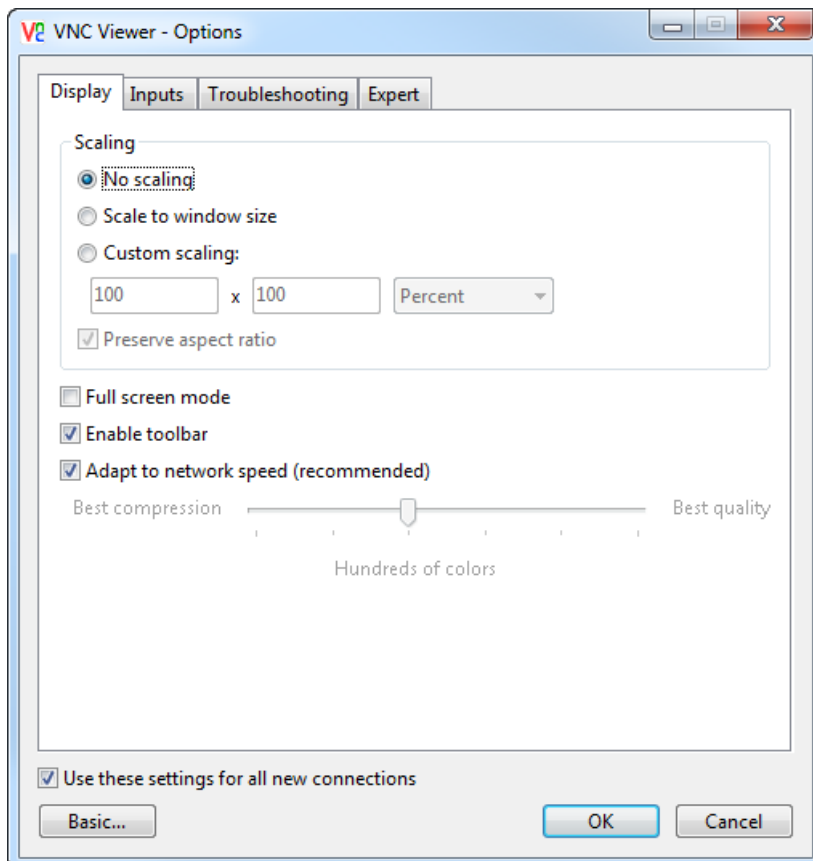
You can quickly close the current connection. To do this, click the **Close Connection**  toolbar button. You are prompted to confirm the operation before the *VNC Viewer* window closes.

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 in 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. *More on this dialog.*



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 as expected.

To toggle full screen mode on and off, click the **Full Screen Mode**  toolbar button. Note scroll bars are not displayed in this mode; bump the mouse against an edge to scroll.

Trading performance for picture quality

You may be able to enhance the performance of the connection by reducing the number of colors used to display the host computer's desktop. To do this, turn off **Adapt to network speed**, 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 and Mac OS X 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 and cause the client computer to be affected by the following keys and key combinations:

- Under Windows, turn off **Pass special keys directly to VNC Server** for WINDOWS (also known as START), PRINT SCREEN, ALT-TAB, ALT-ESCAPE, CTRL-ESCAPE.
- Under Mac OS X, turn off **Pass media keys directly to VNC Server** for VOLUME UP, PLAY, and similar media keys.

Note these options are on the **Inputs** tab.

Disabling the toolbar

You can disable the *VNC Viewer* toolbar. *More on this toolbar.* 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. *More on this menu.* 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 features

By default, while a connection is in progress, you can control the host computer using your keyboard and mouse, and in addition copy and paste text between applications running on the client and host computers.

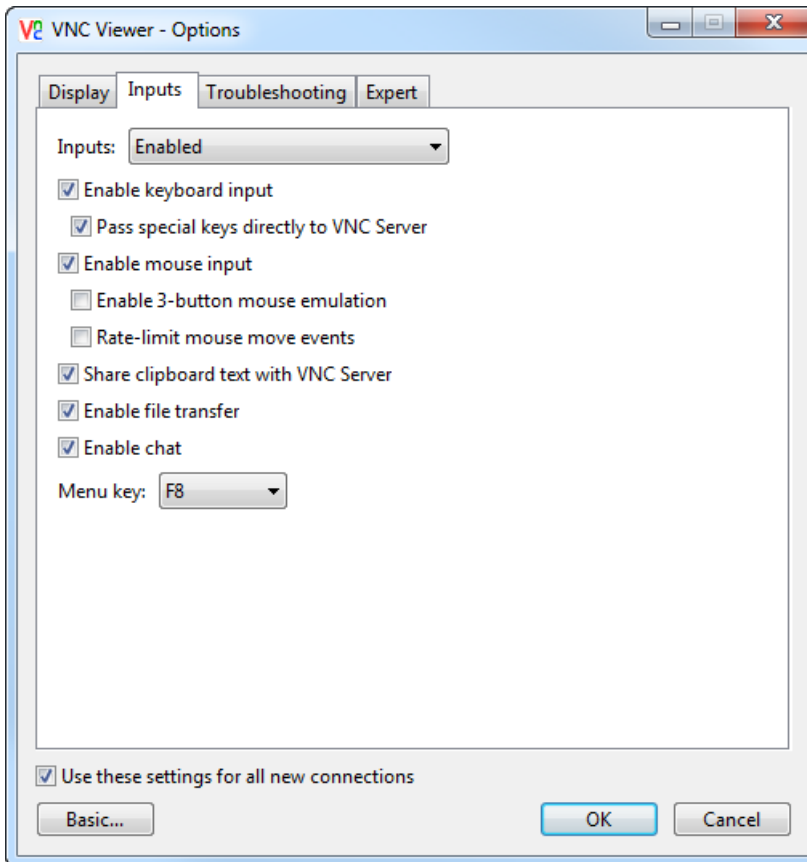
For connections to *VNC Server* with an Enterprise or a Personal license, you can also:

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

Note that:

- *VNC Viewer* might have been configured to disable printing before the connection started; see *Configuring printing* on page 39.
- *VNC Server* may have been configured to prevent some or all of these features; see *Restricting functionality for connected users* on page 110.

You can restrict access to features while the connection is in progress by configuring options on the **Inputs** tab of the **Options** dialog. *More on this dialog.* You might want to do this if you are watching a demonstration on the host computer, for example, and want to prevent inadvertent interruption.



Note: You can enable features 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 46.

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 64*.

Disabling copy and paste text

You can disable copy and paste text 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 68*.

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 69*.

4

Connecting From A Web Browser

This chapter explains how to connect to and control a host computer using *VNC Viewer for Java*. All you need to do this is a Java-enabled web browser with which to download *VNC Viewer for Java* from *VNC Server* with an Enterprise or a Personal license on demand; you do not have to install any software. This may be useful if you are at an Internet café, for example.

Note: *VNC Viewer for Java* is not available to download from *VNC Server* with a Free license.

Once downloaded, you can use the *VNC Viewer for Java* applet to establish a connection in exactly the same way as *VNC Viewer*. You use your mouse and keyboard to control the host computer exactly as you would using *VNC Viewer*.

Note: *VNC Viewer for Java* has considerably fewer remote control features than *VNC Viewer*. For more information, see *Connecting from VNC Viewer for Java* on page 15.

Contents

Connecting to a host computer	52
The VNC Viewer for Java user experience	56
Working with VNC Viewer for Java	57

Connecting to a host computer

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

1. Download *VNC Viewer for Java* from *VNC Server* with an Enterprise or a Personal license running on the host computer you want to connect to. See *Downloading VNC Viewer for Java* on page 52.
2. Use the *VNC Viewer for Java* applet to connect to *VNC Server*. See *Connecting to VNC Server* on page 54.

Downloading VNC Viewer for Java

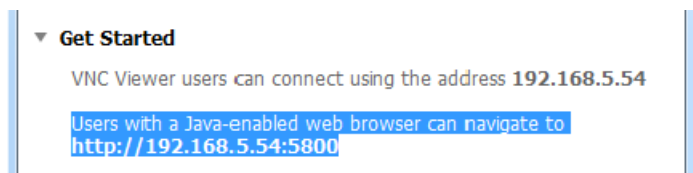
The first stage is to download *VNC Viewer for Java* to your web browser on demand. To do this:

1. Start a Java-enabled web browser on the client computer, for example the latest version of Internet Explorer, Firefox, Safari, or Chrome.

Note: For more information on Java, visit www.java.com. Note that Java (JRE or JDK) 5+ must be installed on the client computer.

2. In the address bar, enter `http://` and the network address of the host computer, qualified by the port number on which *VNC Server* is listening for download requests, for example `http://192.168.5.54:5800`.

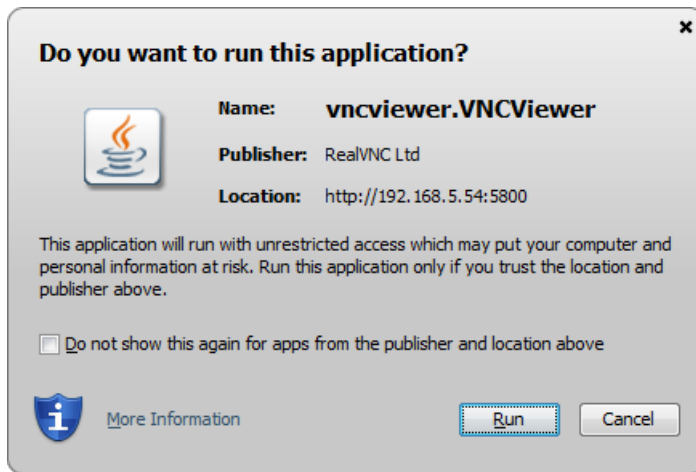
If you do not know a network address for the host computer and you do not have access to it, you will need to consult your system administrator or a host computer user. If you *do* have access to the host computer, and you are connecting within a private network, the information you need is displayed in the **Get Started** section of the **VNC Server** dialog. *More on this dialog.*



Note: 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 28 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 30 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 26.

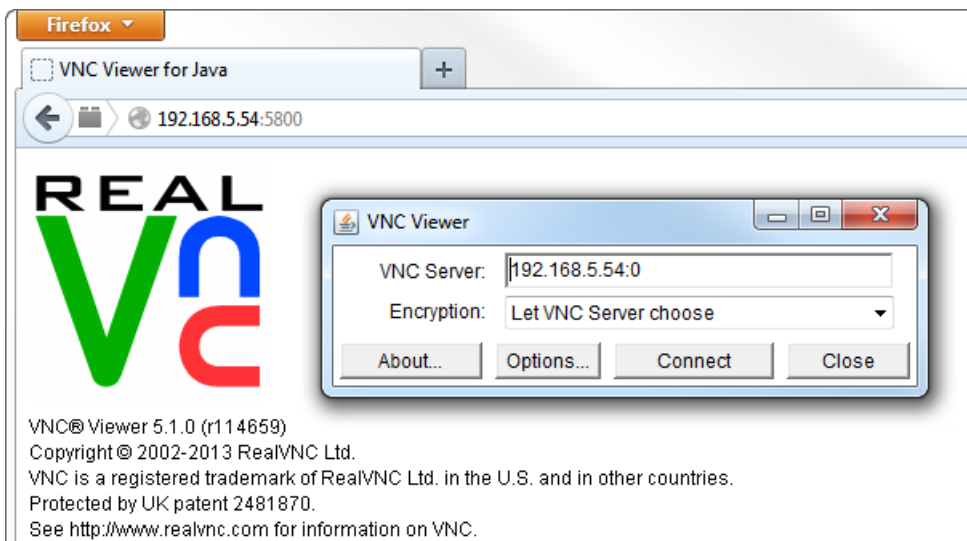
3. If this is the first time you have downloaded *VNC Viewer for Java*, you are prompted to trust it:



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:

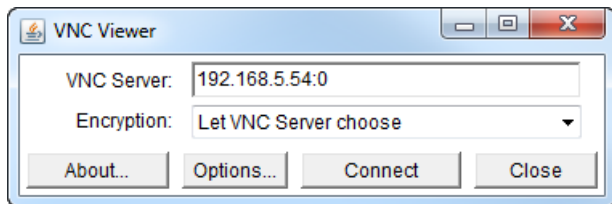


(In this picture, the web browser is Firefox 25. Note that the web browser window must stay open while the connection is in progress.)

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*.

The **VNC Server** dropdown on the **VNC Viewer** dialog displays the network address of the host computer, 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):



For more information on network addresses and port numbers, start with *Step 3: Identify VNC Server running on the host computer on page 21*.

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 encrypted connection on page 22*.
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 55*.
3. Click the **Connect** button.

You may be asked to check the identity of *VNC Server*, acknowledge the encryption status, and authenticate. For more information on these issues, see *Step 5: Connect to VNC Server on page 23*.

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 56*.

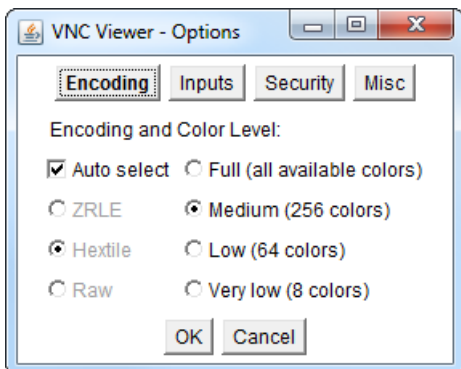
If the connection fails for any reason, start with *Troubleshooting connection on page 26*.

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 58.

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

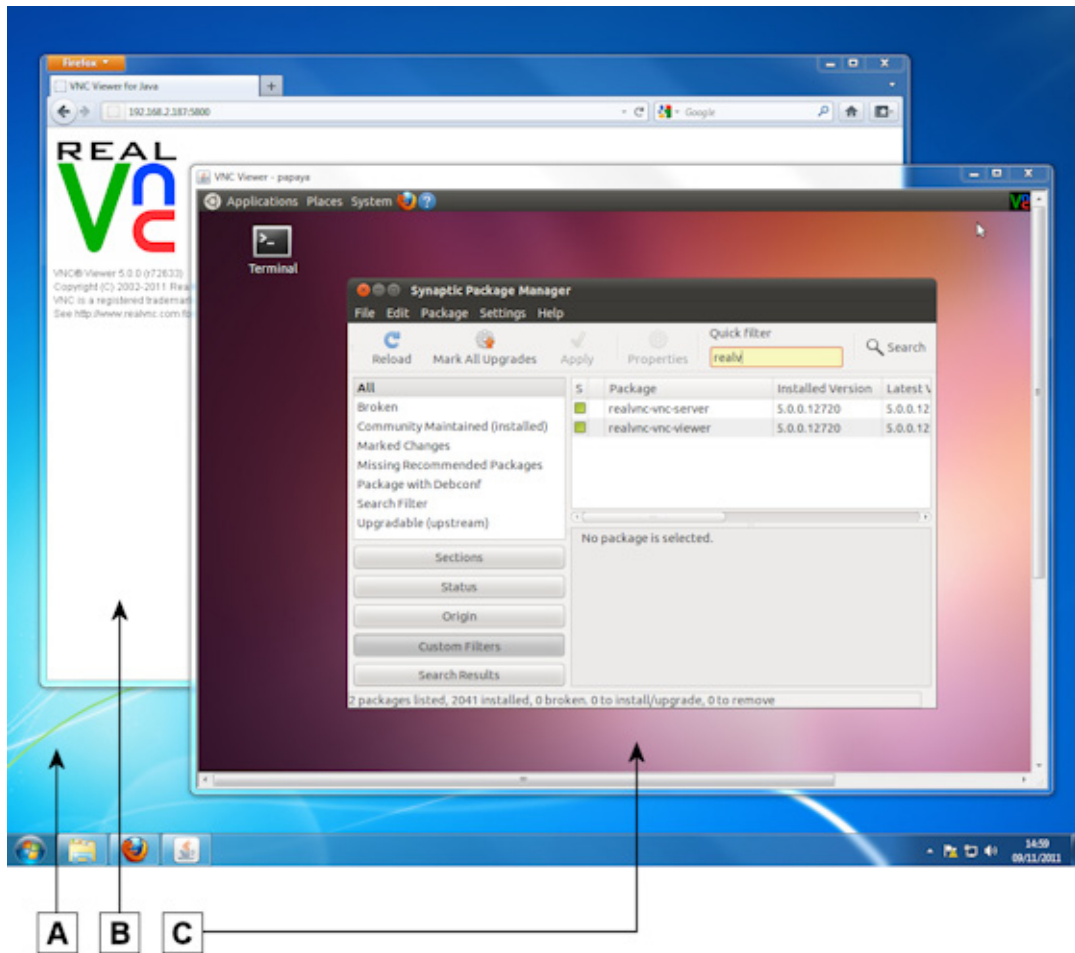


The following options must be configured before a connection is made:

- 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.

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 7. **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 11.04 Linux.

The client computer's mouse and keyboard are now shared with the host computer in exactly the same way as VNC Viewer. For more information, start with *Controlling the host computer using your mouse* on page 41.

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 VNC Viewer for Java on page 15*.

Using the VNC Viewer for Java shortcut menu

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

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

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

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

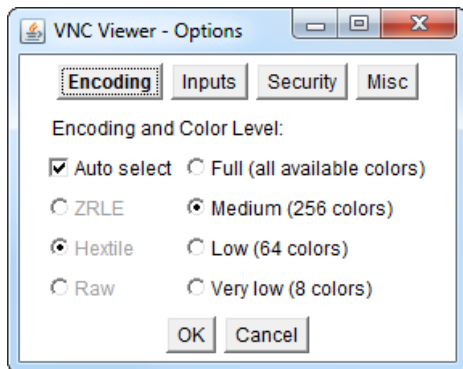
The following table explains the effect of selecting these menu options.

Option	Purpose
Exit VNC Viewer	Close the current connection (and the <i>VNC Viewer for Java</i> window).
Clipboard	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. See <i>Copying and pasting text</i> on page 59. Note that if you chose not to trust <i>VNC Viewer for Java</i> when you downloaded it, you can only copy and paste text between the two computers via this dialog.
Send F8	Send an F8 command to the host computer. (F8 opens the shortcut menu.)
Send Ctrl-Alt-Del	Send the CTRL-ALT-DELETE command to the host computer. (Pressing this key combination would be interpreted by the client computer.)

Option	Purpose
Refresh screen	Refresh the display of the host computer's desktop.
New connection	Start a new connection to the same host computer, or to a different one, using the same web browser session. You do not need to download <i>VNC Viewer for Java</i> again.
Options	Configure most aspects of <i>VNC Viewer for Java</i> while the current connection is in progress. See <i>Using the Options dialog</i> on page 58. Note that some options must be configured before you connect. See <i>Configuring VNC Viewer for Java before you connect</i> on page 55.
Connection info	Display technical information about the current connection, such as the encryption method and compression format. You may need this if you contact Technical Support.
About VNC Viewer	Display information about <i>VNC Viewer for Java</i> . You may need this if you contact Technical Support.
Dismiss menu	Close the shortcut menu.

Using the Options dialog

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



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 55.

To open the **Options** dialog, select **Options** from the shortcut menu. *More on this menu.*

The following sections explain the options in this dialog.

Trading performance for picture quality

You may be able to enhance the performance of *VNC Viewer for Java* by reducing the number of colors used to display the host computer's desktop. To do this, turn off **Auto select** and choose either 256, 64, or 8 colors. These 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 text* on page 59.

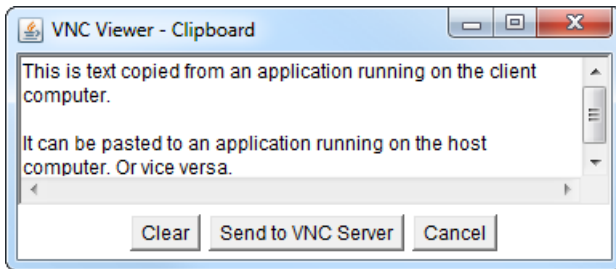
Troubleshooting display

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 text

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 68 for more information.

You can preview the contents of the Clipboard to see what text is available to paste. To do this, select **Clipboard** from the *VNC Viewer for Java* shortcut menu. *More on this menu*. The **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. *More on this dialog*. 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.

5

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.

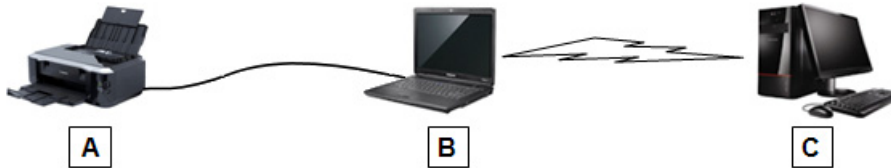
Note: Not all features are available for connections to *VNC Server* with a Free license. For a summary, see *Connecting to VNC 5.x* on page 13.

Contents

Printing host computer files to a local printer	62
Transferring files between client and host computers	64
Copying and pasting text between client and host computers	68
Communicating securely using chat	69

Printing host computer files to a local printer

If you are connected to *VNC Server* with an Enterprise or a Personal license, 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 the client's default printer. **C.** Host computer running VNC Server, and storing the files to print.

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

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

A best possible quality print finish is attempted. 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 62.

If the host computer file does not print to the local printer, start with *Troubleshooting printing* on page 63.

Disabling and enabling printing

You may be allowed to disable printing providing you do so before you connect. Open the **Options** dialog and, on the **Printing** tab, choose **Don't share a printer**. *More on this dialog.*

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 > Devices and Printers** under Windows 7.

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 you connected to *VNC Server* with an Enterprise or a Personal license? You cannot print when connected to *VNC Server* with a Free license. For more information, see *Connecting to VNC 5.x* on page 13.
2. If you are using a previous version of *VNC Viewer* or *VNC Server*, is it at least version 4.5? Printing is not supported by earlier versions.
3. Are both client and host computers running supported operating systems? Printing is not supported to or from certain platforms, including HP-UX, AIX, and Windows NT 4; in addition, prior configuration is required in order to print to or from Solaris 9 and 10, SUSE Linux, and systems with SE Linux enabled. For the latest information, visit www.realvnc.com/products/vnc/documentation/latest/misc/printing/.
4. If the host computer is running Linux or Mac OS X, is CUPS version 1.3 or later installed? For more information, consult the host computer's operating system documentation.
5. Is the local printer connected to the client computer? Is it switched on? Is it ready to print? Does it have paper? Is it set as the client computer's default printer?
6. Has *VNC Viewer* been configured to disable printing? To see how to enable it again, read *Disabling and enabling printing* on page 62. You will have to close the current connection and then reconnect.
7. Has *VNC Viewer* 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 62. 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 must always explicitly select your local printer when you print.

If you have to explicitly select your 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.

8. Has *VNC Server* been configured to disable 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 allowed to enable it again; see *Restricting functionality for all connected users* on page 111.
9. Has *VNC Server* 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; see *Restricting functionality for particular connected users* on page 112.


Transferring files between client and host computers

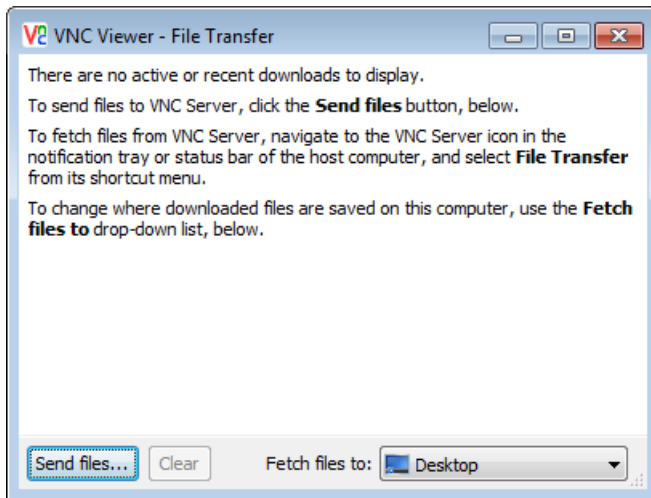
If you are connected to *VNC Server* with an Enterprise or a Personal license, you can exchange files with the host computer.

Note: If file transfer fails for any reason, see *Troubleshooting file transfer* on page 67.

Sending files to a host computer

To send files to a host computer:

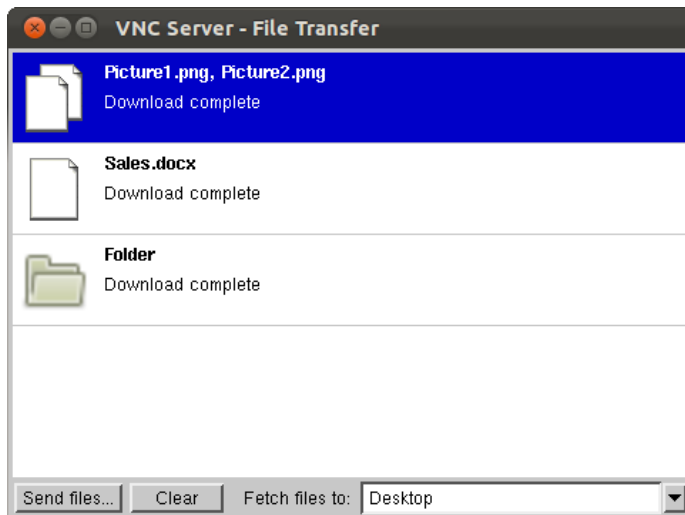
1. Click the **File Transfer**  *VNC Viewer* toolbar button. The **File Transfer** dialog opens on the client computer:



2. Click the **Send files** button. The **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). The **File Transfer** dialog opens on the host computer:




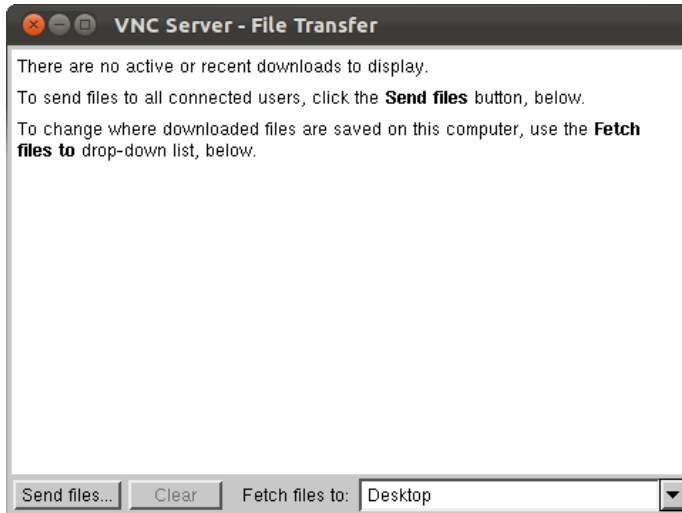
The most recent file transfer operation is highlighted. You can check its status, or pause or stop the transfer if it takes more than a few seconds.

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** dialog. Note you must have write permissions for the folder you choose. Alternatively, you can ask to be prompted each time.

Publishing files to all connected client computers

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

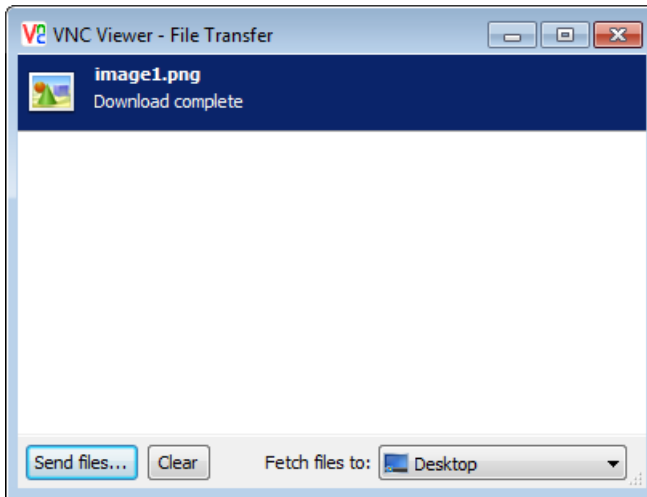
1. In the *VNC Viewer* window, right-click the *VNC Server* icon  (typically shaded black) and, from the shortcut menu, select **File Transfer**. *More on this icon*. The **File Transfer** dialog opens on the host computer:



2. Click the **Send files** button. The **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.

- Click **Open** (**OK** under UNIX). The **File Transfer** dialog opens on the client computer:




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** 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 may be allowed to 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**. *More on this dialog.* The **File Transfer**  **VNC Viewer** toolbar button is disabled.

If you were allowed to disable file transfer, you can enable it again at any time.

Troubleshooting file transfer

If file transfer does not work, check the following:

1. Are you connected to *VNC Server* with an Enterprise or a Personal license? You cannot transfer files to or from *VNC Server* with a Free license. For more information, see *Connecting to VNC 5.x* on page 13.
2. If you are using a previous version of *VNC Viewer* or *VNC Server*, is it at least version 4.4? File transfer is not supported by earlier versions.
3. Has *VNC Viewer* been configured to disable file transfer? To see how to enable it again, read *Disabling and enabling file transfer* on page 67.
4. Has *VNC Server* been configured to disable 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 allowed to enable it again; see *Restricting functionality for all connected users* on page 111.

5. Has *VNC Server* 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; see *Restricting functionality for particular connected users* on page 112.

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: The computer you are pasting to must support the language of the copied text in order for it to be pasted meaningfully. In addition, any formatting applied to the copied text, such as italics, will be lost.

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` for a Mac OS X host computer, 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` for a Mac OS X host computer, 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 text fails for any reason, start with *Troubleshooting copy and paste text* on page 68.

Disabling and enabling copy and paste text

You may be allowed to disable copy and paste text 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**. *More on this dialog.*

If you were allowed to disable copy and paste text, you can enable it again at any time.

Troubleshooting copy and paste text

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


1. Has *VNC Viewer* been configured to disable copy and paste text? To see how to enable it again, read *Disabling and enabling copy and paste text* on page 68.

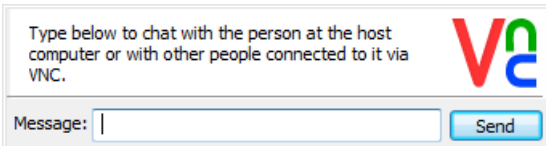
2. Has *VNC Server* been configured to disable copy and paste text? If this is the case and you do not have access to the host computer, you will need to consult your system administrator or a host computer user. If you *do* have access to the host computer, and sufficient privileges to configure *VNC Server*, you may be allowed to enable it again; see *Restricting functionality for all connected users* on page 111.
3. Has *VNC Server* been configured to prevent *you* copying and pasting text? 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; see *Restricting functionality for particular connected users* on page 112.
4. Does the amount of text being copied and pasted exceed 256kB? If so, the entire paste operation fails, and the last text copied to the Clipboard is pasted instead.

Communicating securely using chat

If you are connected to *VNC Server* with an Enterprise or a Personal license, 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: If you cannot use chat for any reason, see *Troubleshooting chat* on page 71.

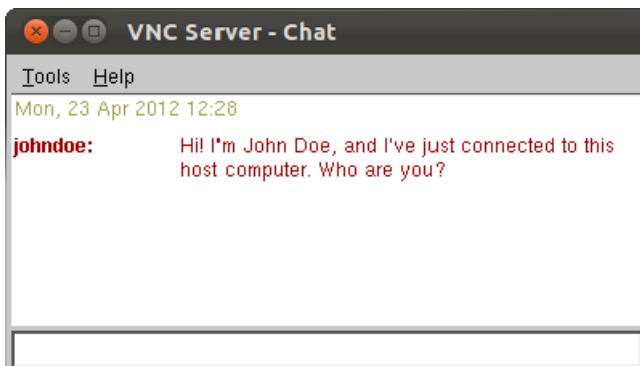
To participate in a conversation, or start a new one, click the **Start Chat Session**  *VNC Viewer* toolbar button. A message box appears at the bottom of the *VNC Viewer* window:



Type below to chat with the person at the host computer or with other people connected to it via VNC.

Message:

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



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.

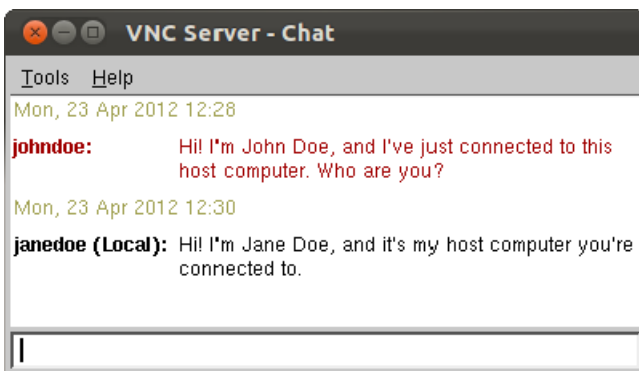
Chatting as a host computer user

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. *More on this menu.*
2. Select **Chat**. The **Chat** dialog opens. Type text in the field at the bottom:



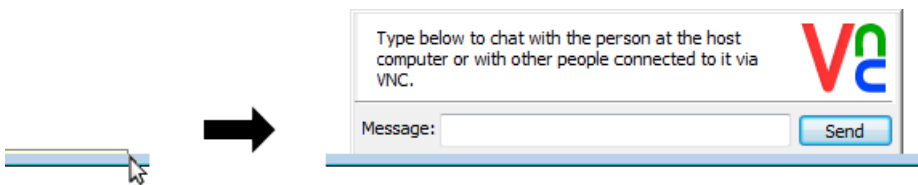
3. Press the ENTER key to send the message:



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

Working with chat

The 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:



Note that the **Chat** dialog can also be minimized. If so, you are notified when new messages appear by the taskbar button flashing (Windows and UNIX) 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** 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 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 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** dialog.

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**. *More on this dialog.* The

Start Chat Session  *VNC Viewer* toolbar button is disabled.

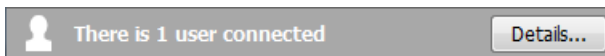
Note: Chat is only disabled for you, and not for any other connected *VNC Viewer* user. You can still view messages in the **Chat** dialog.

You can enable chat again at any time.

Troubleshooting chat

If you cannot use chat, check the following:

1. Are you connected to *VNC Server* with an Enterprise or a Personal license? You cannot chat to users of *VNC Server* with a Free license. For more information, see *Connecting to VNC 5.x* on page 13.
2. If you are using a previous version of *VNC Viewer* or *VNC Server*, is it at least version 4.5? Chat is not supported by earlier versions.
3. Is there anyone to chat with? The **VNC Server** dialog reveals if any *VNC Viewer* users are connected. *More on this dialog.*



4. Has *VNC Viewer* been configured to disable chat? To see how to enable it again, read *Disabling and enabling chat* on page 71.
5. Has *VNC Server* been configured to disable 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 allowed to enable it again; see *Restricting functionality for all connected users* on page 111.
6. Has *VNC Server* 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; see *Restricting functionality for particular connected users* on page 112.

6

Working With VNC Server

Once licensed, *VNC Server* enables 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 operate *VNC Server*. It also explains advanced scenarios such as running concurrently and in different modes, configuring ports, and troubleshooting. For comprehensive security information, see *Chapter 7, Making Connections Secure* on page 95.

This chapter assumes you have access to the host computer and sufficient privileges to configure both it and *VNC Server*. Note that if you are setting up *VNC Server* for unattended access, some features require a host computer user to be present when a connection is established, and are therefore not recommended.

Contents

Licensing VNC Server	74
Starting VNC Server	75
Running VNC Server	78
The VNC Server user interface	82
Troubleshooting VNC Server	87
Configuring VNC Server	89
Changing ports	90
Notifying when users connect	92
Stopping VNC Server	93

Licensing VNC Server

VNC Server must be licensed. If it is not, users cannot connect.

For more information on the different license types available, to compare the remote control features provided by each, and to obtain a free, paid, or trial license key, visit www.realvnc.com/products/vnc/licensing/.

Applying a license key

You can apply a license key to *VNC Server* at any time.

You typically first do this when you download and install *VNC Server*. You may subsequently apply a key in order to renew your support and upgrades contract, or to add a feature.

1. Open the *VNC Server* shortcut menu. *More on this menu.*
2. Choose **Licensing**. The **Licensing** dialog opens.
3. Follow the instructions. Note you may additionally be prompted to configure *VNC Server*; see *Repairing VNC Server on page 74* for more information.

Alternatively, you can apply a license key:

- At the command line using the `vnclicense` utility; start with www.realvnc.com/products/vnc/documentation/latest/reference/vnclicense.html.
- Remotely to Windows computers by deploying the *VNC Server* MSI using Group Policy; visit www.realvnc.com/products/vnc/deployment/msi/.
- Remotely to any supported computer by setting policy; visit www.realvnc.com/products/vnc/deployment/policy/.
- Centrally for UNIX computers by hosting *VNC Server* on a network share; see *Hosting VNC on a UNIX network share on page 144*.

Repairing VNC Server

When you apply a license key you may additionally be prompted to repair *VNC Server*. This is typically because your license key entitles you to fewer RealVNC remote control features than *VNC Server* is currently configured to use. You must harmonize *VNC Server* with the license key.

For example, if at the end of a trial of an Enterprise or a Personal license you choose to downgrade to a Free license, you must turn off encryption and system authentication. If you do not, users cannot connect.

Note it is possible to run more than one instance of *VNC Server* on a host computer; see *Running VNC Server on page 78*. If this is the case, you must repair all running instances separately. For example, if under UNIX you have five instances of *VNC Server* running, two in User Mode and three in Virtual Mode, and you apply the new license key to a particular instance of User Mode, then you must separately configure:

- The other instance of User Mode.
- All three instances of Virtual Mode.

Until you do, users will only be able to connect to these instances for a limited time.

Note that administrative privileges may be required to perform this operation if you are not the user starting *VNC Server*.

Understanding license scope

Under Windows, a *VNC Server* license key is system-wide. This means that it applies across all user accounts on the host computer. Since only two instances of *VNC Server* can run concurrently on a Windows computer (one in Service Mode, and one in User Mode for the currently logged on user account), this means that *VNC Server* is always licensed for all users.

Under UNIX and Mac OS X, however, there is another dimension to license scope. The license to use *VNC Server* not only applies to all user accounts, but additionally limits the number of instances of *VNC Server* you can start. For example, if your license entitles you to five 'desktops', attempting to start *VNC Server* for a sixth time fails. For more information, visit www.realvnc.com/products/vnc/documentation/latest/licensing-faq/.

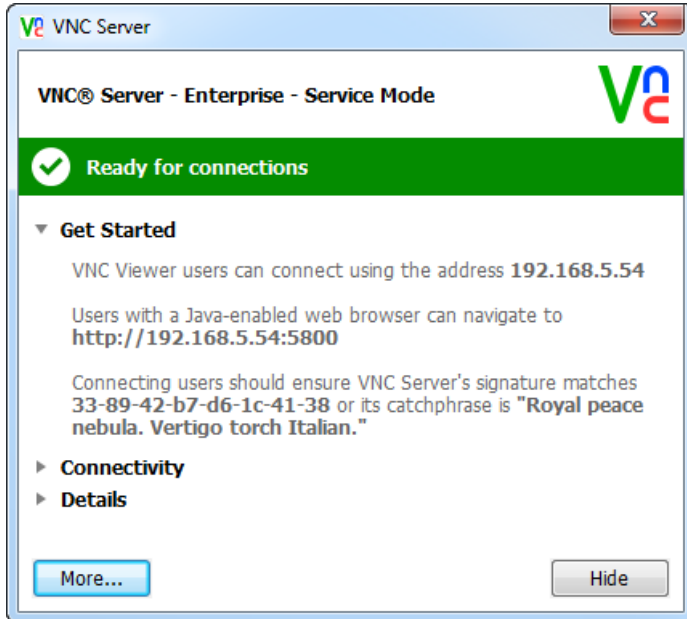
Note: You can quickly see how many instances of *VNC Server* your license permits you to start, and how many are currently running. See page 79 for more information.

Note you can start a maximum of five instances of *VNC Server* on UNIX and Mac OS X computers with a Free or a trial license. Upgrade to an Enterprise or a Personal license if flexibility is important to you.

Starting VNC Server

Depending on the platform and your license, you can start *VNC Server* more than once on a host computer, perhaps in different modes. For more information about modes, which you might want to use, and why you might want to run more than one instance of *VNC Server*, see *Running VNC Server on page 78*.

To see how to start *VNC Server*, follow the platform-specific instructions below. In most circumstances, a **VNC Server** dialog appears:



(In this picture, VNC Server is running in Service Mode under Windows.)

The **VNC Server** dialog is the gateway to VNC Server and all its features. *More on this dialog.*

To see how to stop VNC Server, or to learn why VNC Server might stop automatically, read *Stopping VNC Server* on page 93.

Windows

To start VNC Server in:

- Service Mode, search for or navigate to **VNC Server**, or run the appropriate command from www.realvnc.com/products/vnc/documentation/latest/reference/vncserver-operations.html (administrative privileges are required).

Note: By default, VNC Server automatically starts as a service when the computer is powered on. If you explicitly stop VNC Server, however, the service does not restart when the computer is rebooted.

- User Mode, search for or navigate to **VNC Server (User Mode)**, or run the appropriate command (see www.realvnc.com/products/vnc/documentation/latest/reference/vncserver-operations.html).

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

UNIX

To start *VNC Server* in:

- User Mode, search for or navigate to **VNC Server (User Mode)**, or run the appropriate command (see www.realvnc.com/products/vnc/documentation/latest/reference/vncserver-operations.html).
- Service Mode, run the appropriate command for your system, for example `/etc/init.d/vncserver-x11-serviced start` or `systemctl start vncserver-x11-serviced.service`. Typically, it is useful to have this service start automatically when the computer powers on; visit www.realvnc.com/products/vnc/documentation/latest/reference/vncserver-x11-serviced.html for more information.
- Virtual Mode, run the command `vncserver-virtual`. Note you should *not* do this with elevated privileges. No user interface is available to help you work with *VNC Server* in this mode; instead, a message is printed to the console. See *Working with VNC Server in Virtual Mode on page 80* for more information.

Note: If you have an Enterprise license, you can run *VNC Server* in Virtual Mode as a service, in which case a new instance is started automatically, and a virtual desktop created, on demand. See *Creating virtual desktops on demand on page 81* for more information.

Mac OS X

To start *VNC Server* in:

- Service Mode, search for or navigate to **VNC Server**, or run the appropriate command from www.realvnc.com/products/vnc/documentation/latest/reference/vncserver-operations.html (elevated privileges are required).

Note: *VNC Server* in Service Mode automatically starts when the computer powers on.

- User Mode, search for or navigate to **VNC Server (User Mode)**, or run the appropriate command (see www.realvnc.com/products/vnc/documentation/latest/reference/vncserver-operations.html).

Running VNC Server

Under any platform, and providing your license entitles you 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 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, in different states and for different purposes.

To...	Run VNC Server in...	Platforms	Connected users see...
Remote the console of the host computer	Service Mode	All	Exactly what a person sitting in front of the host computer would see. This is either the desktop of a user account if one is currently logged on, or the Login screen if not. Note <i>VNC Server</i> is typically set to start when the system powers on, and users can connect and reconnect until <i>VNC Server</i> is explicitly stopped.
Remote the desktop of the currently logged-on user account	User Mode	All	Exactly what a person sitting in front of the host computer would see <i>while the current user account is logged on</i> . When this user account is logged off, <i>VNC Server</i> automatically stops, users are disconnected, and cannot reconnect. Note the Login screen is not available to connected users.
Create and remote a virtual desktop	Virtual Mode	UNIX	<p>A <i>virtual desktop</i>, created when <i>VNC Server</i> is started and not destroyed until <i>VNC Server</i> is explicitly stopped. Connected users therefore do <i>not</i> see what a person sitting in front of the host computer would see; neither the desktop of the currently logged on user account, nor the Login screen, are available. Instead, connected users gain a private workspace to which they can connect and reconnect until <i>VNC Server</i> is explicitly stopped. See <i>Working with VNC Server in Virtual Mode on page 80</i>.</p> <p>With an Enterprise license, you can run <i>VNC Server</i> in Virtual Mode as a <i>service</i>, which means virtual desktops can be created <i>on demand</i>. These virtual desktops, however, do <i>not</i> persist. See <i>Creating virtual desktops on demand on page 81</i>.</p>

VNC Server can run in Service Mode and User Mode concurrently, though this is not generally useful, and likely to result in port conflicts. See *Changing ports on page 90* for more information.

Under UNIX, *VNC Server* is designed to run in Virtual Mode as many times as your license has available ‘desktops’. It can safely be run concurrently with either other mode.

For platform-specific information, see the sections below. To see how to start *VNC Server* in different modes, read *Starting VNC Server on page 75*.

Windows

You can start *VNC Server* a maximum of twice on a host computer; once in Service Mode, and once in User Mode for the currently logged on user account.

Note: Microsoft User Account Control severely restricts users connected to *VNC Server* in User Mode from fully controlling a host computer running Windows Vista or later. The 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), and can only continue if a host computer user closes the program, or accepts the prompt.

Once connected to *VNC Server* in either mode, a user has the same privileges (that is, access rights) on the host computer as the *currently logged on user account*. This need not be a user with administrative privileges even if the credentials of one were supplied in order to authenticate to *VNC Server*; see *Authenticating users on page 96* for more information. The opposite also holds true: a connected user has administrative privileges if such a user account is currently logged on.

UNIX

You can start *VNC Server* as many times as your license permits. Each time you do, one 'desktop' is decremented from your license. To see how many are left, run the command `vnclicense -check`. For example:

```
Licensed desktops: 5
Running desktops: 3
    johndoe: 2
    janedoe: 1
```

This means that five desktops are licensed to run concurrently on the 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 re-increment your license by killing desktops. To see how to do this, read *Stopping VNC Server on page 93*.

You can start *VNC Server* once in Service Mode. You can start *VNC Server* once in User Mode for the currently logged on user account. And you can start *VNC Server* in Virtual Mode to create as many virtual desktops as you need.

Once connected to *VNC Server* in:

- User Mode or Service Mode, a user has the same privileges (that is, access rights) on the host computer as the *currently logged on user account*. This need not be a user with administrative privileges even if the credentials of one were supplied in order to authenticate to *VNC Server*; see *Authenticating users on page 96* for more information. The opposite also holds true: a connected user has administrative privileges if such a user account is currently logged on.
- Virtual Mode, a user has the same privileges as the host computer user starting *VNC Server*, irrespective of whether or not a user account is currently logged on.

Mac OS X

You can start *VNC Server* as many times as your license permits. Each time you do, one 'desktop' is consumed from your license. To see how many are left, run the command `/Library/vnc/vnclicense -check`; see the UNIX section above for an explanation of the output.

You can start *VNC Server* once in Service Mode. You can start *VNC Server* once in User Mode for the currently logged on user account. And you can start *VNC Server* in User Mode for other user accounts providing Fast User Switching is turned on, and the `StopUserModeOnSwitchOut` VNC parameter is set to `False`. Visit www.realvnc.com/products/vnc/documentation/latest/parameters/vncserver.html#stopusermodeonswitchout for more information.

Once connected to *VNC Server* in either mode, a user has the same privileges (that is, access rights) on the host computer as the *currently logged on user account*. This need not be a user with administrative privileges even if the credentials of one were supplied in order to authenticate to *VNC Server*; see *Authenticating users on page 96* for more information. The opposite also holds true: a connected user has administrative privileges if such a user account is currently logged on.

Working with VNC Server in Virtual Mode

Note: The information in this section applies to UNIX platforms only.

When *VNC Server* in Virtual Mode starts, a *virtual desktop* is created, independent of the console and detached from any physical display hardware. This means that desktop artifacts such as the *VNC Server* icon and **VNC Server** dialog are not available to help you work with *VNC Server*. For more information, visit www.realvnc.com/products/vnc/documentation/latest/reference/vncserver-virtual.html.

Managing the virtual desktop environment

When VNC is installed, a default system-wide `/etc/vnc/xstartup` file is created, specifying a window manager and other settings for all virtual desktops created for all user accounts on that computer. This file is reserved for use by RealVNC.

To specify a different window manager, start particular applications, or manage any other aspect of the virtual desktop environment, create `/etc/vnc/xstartup.custom` and make it executable. This file will be executed in preference to `/etc/vnc/xstartup`.

To specify a virtual desktop environment for a particular user account, create `~/.vnc/xstartup` and make it executable. This file will be executed in preference to a system-wide file for all virtual desktops created for that user account only.

Connecting to VNC Server in Virtual Mode

A virtual desktop is assigned an X Window System display number corresponding to the port on which *VNC Server* is listening for connection requests. When *VNC Server* starts, a message ending with text similar to the following is printed to the Terminal window:

```
New desktop is johndoe:1 (192.168.0.187:1)
```

In this example, display number 1 has been automatically assigned, corresponding to port 5901. To assign a particular display number, declare it explicitly, for example:

```
vncserver-virtual :2
```

Configuring VNC Server in Virtual Mode

You can:

- Specify VNC parameters in appropriate VNC configuration files, or at the command line when you start *VNC Server*. See *Specifying VNC parameters on page 130* for more information.
- Configure *VNC Server* as a connected user. To do this, start *VNC Viewer* and supply the network address and display number (see the example output above). Once connected, (virtual) desktop artifacts are available to help you work with *VNC Server*. See *The VNC Server user interface on page 82* for more information.

Creating virtual desktops on demand

If you have an Enterprise license, you can run *VNC Server* in Virtual Mode as a *service*, to create virtual desktops on demand. Note this service listens on port 5999 by default. For more information, visit www.realvnc.com/products/vnc/documentation/latest/reference/vncserver-virtuald.html.

For example, if you run the service on a computer `acmecorp` and a connecting user successfully authenticates using the credentials of the user account John Doe, then:

1. An instance of *VNC Server* in Virtual Mode is automatically started, and an `acmecorp:1` virtual desktop is created.
2. The newly-connected user is transferred to, and can immediately control, `acmecorp:1`.
3. One desktop is decremented from your license.
4. `acmecorp:1` is destroyed (and your license re-incremented) when the user disconnects; a session does not persist.

If a second user authenticates by supplying the credentials of John Doe, an `acmecorp:2` virtual desktop is created, and a second desktop is decremented from your license.

To start the service, run the appropriate command for your system, for example `/etc/init.d/vncserver-virtuald start` or `systemctl start vncserver-virtuald.service`. Typically, it is useful to have it start automatically when the computer powers on.

Note that no desktop artifacts are available to help you work with the service once it has started. To configure it, specify VNC parameters in appropriate VNC configuration files; see *Specifying VNC parameters on page 130* for more information. In particular, note the credentials of *any* user account valid to log on to the host computer can be used to authenticate out-of-the-box. To restrict which users can connect, specify the `Permissions` VNC parameter.

Keeping VNC Server up-to-date

VNC Server can automatically check for:

- Critical security patches.
- Product updates to which you are entitled, if you have an Enterprise or a Personal license and a valid support and upgrades contract; see *Contacting Technical Support on page 8*.

If any appropriate downloads are detected, you are directed to visit the RealVNC web site.

Note: This is a secure web service and no personally identifiable information is collected or stored.

The first time you start *VNC Server*, you are asked whether you would like an automatic check to occur daily. You can subsequently edit your choice on the **Updates** page of the *VNC Server Options* dialog. *More on this dialog.*

To alter the frequency of the update check, specify the `UpdateCheckFrequencyDays` *VNC Server* parameter.

In addition, or alternatively, users can perform a manual check by selecting **Check for updates** on the *VNC Server* shortcut menu. *More on this menu.*

The VNC Server user interface

This section explains key desktop artifacts enabling you to work with *VNC Server*:


- *The VNC Server icon on page 82*
- *The VNC Server shortcut menu on page 83*
- *The VNC Server dialog on page 84*

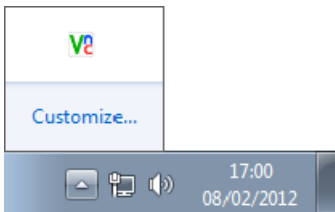
Other desktop artifacts are explained in subsequent sections in this chapter.

Note: Under UNIX, for *VNC Server* in Virtual Mode, desktop artifacts are only available to a *connected* user. For more information, see *Working with VNC Server in Virtual Mode on page 80*.

The VNC Server icon

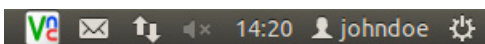
While *VNC Server* is running, an icon  is displayed:

- Under Windows, in the Notification area. Under Windows 7, this is hidden by default and accessible only from  to the right of the Taskbar:



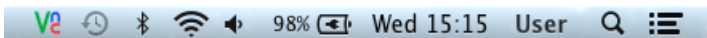
Under Windows XP, the icon may be hidden by other icons. Under Windows 8, the icon is not available on the Start screen, only the Desktop application.

- Under UNIX, in the Notification Area:





Note: Some versions of UNIX are not able to display a *VNC Server* icon.

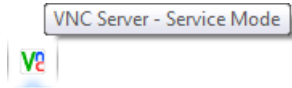
- Under Mac OS X, on the Status Bar:



The *VNC Server* icon:

- Provides visual confirmation that *VNC Server* is running. If the icon is not available, then typically *VNC Server* is not running.
- Provides visual confirmation that *VNC Server* is configured correctly. If not, a red error glyph  appears. Open the **VNC Server** dialog to begin diagnosing the problem. *More on this dialog.*
- Confirms whether users are connected or not. When the first user connects, the icon is shaded black . When the last user disconnects, the icon reverts color again.

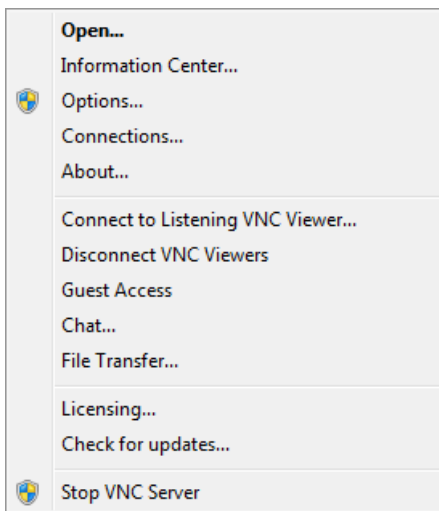
- Provides convenient notification of the mode. Hover the mouse cursor over the icon:



- Has a shortcut menu that performs useful operations. *More on this menu.*

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. *More on this icon.*



(Note that menu options are disabled if they are not available.)

Note: The shortcut menu is also available from the **More** button on the **VNC Server** dialog. *More on this dialog.*

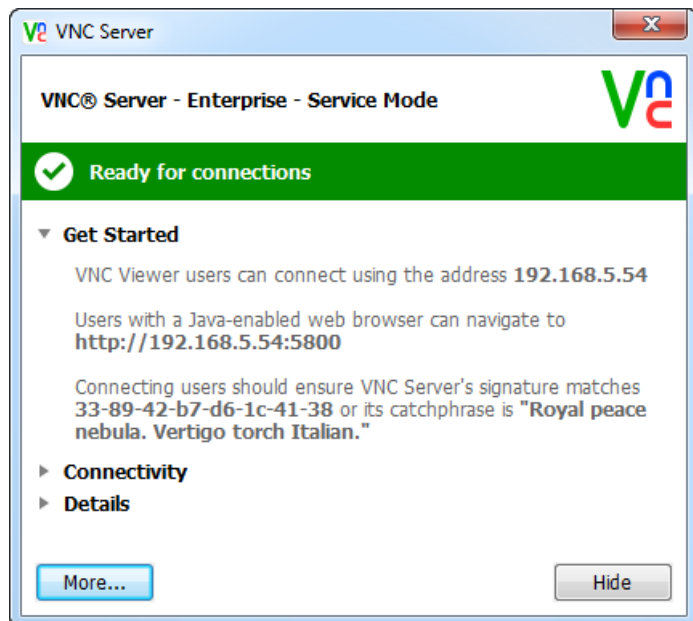
The following table explains the purpose of each shortcut menu option.

Option	Purpose
Open	Work with VNC Server. See <i>The VNC Server dialog</i> on page 84.
Information Center	Understand and resolve issues affecting VNC Server, and retrieve system diagnostics. See <i>Troubleshooting VNC Server</i> on page 87.
Options	Configure VNC Server. Note administrative privileges are required for VNC Server in Service Mode. See <i>Troubleshooting VNC Server</i> on page 87.
Connections	Identify connected users. See <i>Identifying connected users</i> on page 86.
About	See version and trademark information, and a list of open source dependencies.
Connect to Listening VNC Viewer	Establish a reverse connection in conjunction with a client computer user. See <i>Establishing a reverse connection</i> on page 102.

Option	Purpose
Disconnect VNC Viewers	Disconnect all users. Note that, by default, users can immediately reconnect.
Guest Access	When turned on, and providing VNC Server is configured correctly, a Guest is allowed to connect, bypassing VNC Server's authentication scheme. See <i>Allowing a Guest to connect on page 103</i> . Not available for VNC Server with a Free license.
Chat	Chat with all connected users. See <i>Communicating securely using chat on page 69</i> . Not available for VNC Server with a Free license.
File Transfer	Send files to all connected users. See <i>Transferring files between client and host computers on page 64</i> . Not available for VNC Server with a Free license.
Licensing	Apply a license key to VNC Server. See <i>Licensing VNC Server on page 74</i> .
Check for updates	Check for critical security patches and product updates. See <i>Keeping VNC Server up-to-date on page 81</i> .
Stop VNC Server	Stop VNC Server, disconnecting all users. Note administrative privileges are required for VNC Server in Service Mode. See also <i>Stopping VNC Server on page 93</i> .

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:



To open the **VNC Server** dialog, click its taskbar entry in the normal way for a program, or select **Open** from the *VNC Server* shortcut menu. *More on this menu.*

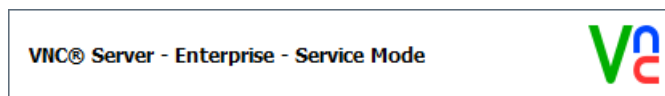
The **VNC Server** dialog:

- Confirms the license type and mode. See *Confirming key information on page 85.*
- Reveals whether *VNC Server* is ready to accept connections. See *Troubleshooting VNC Server on page 87.*
- Provides information to help users connect. Start with *Getting users connected on page 85.*
- Displays the *VNC Server* catchphrase and signature. See *Uniquely identifying VNC Server on page 86.*
- Identifies any connected users. See *Identifying connected users on page 86.*
- Shows expiry dates for trials or support contracts. See *Showing expiry dates on page 87.*

Note: The **VNC Server** dialog also has a **More** button providing access to the same features as the *VNC Server* shortcut menu. *More on this menu.*

Confirming key information

The status bar confirms the license type and mode:

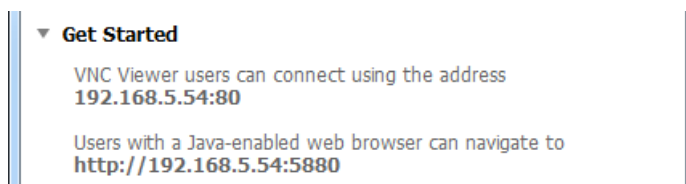


You can apply a license key at any time. See *Licensing VNC Server on page 74* for more information.

For more information on modes, start with *Running VNC Server on page 78.*

Getting users connected

The **Get Started** section contains key information intended to get prospective users quickly connected to *VNC Server* over a private network (for equivalent information for Internet connections, see *Connecting over the Internet on page 28.*) You can select this text and right-click to copy and paste into an email or similar:



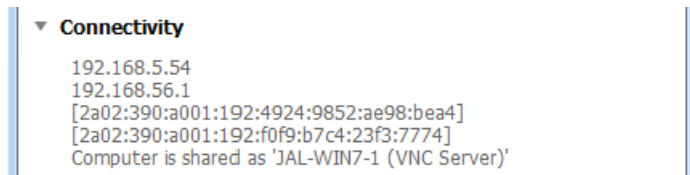
In this picture, *VNC Server* is running on a host computer with a private network address of 192.168.5.54. In addition:

- *VNC Server* is listening for connections on port 5980. The port number is separated from the network address by a single colon, which means it represents a port in the range 5901 to 5999. Note that:
 - If the port number is separated from the network address by two colons, it represents a port outside the range 5900 to 5999, so for example 192.168.5.54::80 means *VNC Server* is listening on port 80.
 - If no port number is displayed, *VNC Server* is listening on the default port for VNC, 5900.
- *VNC Server* with an Enterprise or a Personal license is serving *VNC Viewer for Java* on port 5880.

For more information on ports, start with *Changing ports on page 90*.

Listing all connectivity information

The **Connectivity** section lists all network addresses and other means of connecting to *VNC Server* over a private network (for equivalent information for Internet connections, see *Connecting over the Internet on page 28*):

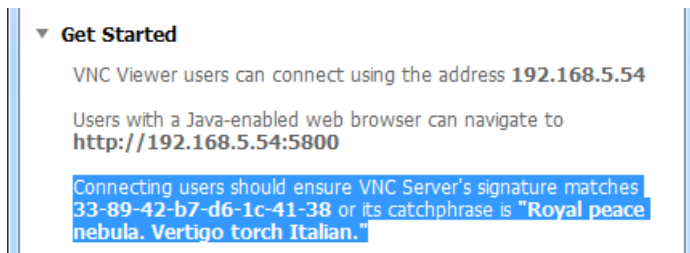


In this picture:

- Two IPv4 network addresses are available.
- Two IPv6 network addresses are available. Note these are only valid in an IPv6-enabled environment.
- The Bonjour or Avahi name is displayed. Note only Zeroconf-enabled applications such as *VNC Viewer for Android* or *VNC Viewer for iOS* are able to discover *VNC Server*; *VNC Viewer* is not Zeroconf-enabled in this release. Note this feature is also not available with a Free license.

Uniquely identifying VNC Server

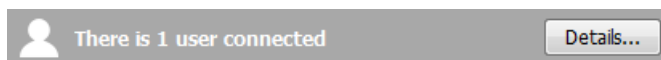
For *VNC Server* with an Enterprise or a Personal license, the **Get Started** section displays a catchphrase (and the less-memorable signature on which it is based) uniquely identifying *VNC Server*:



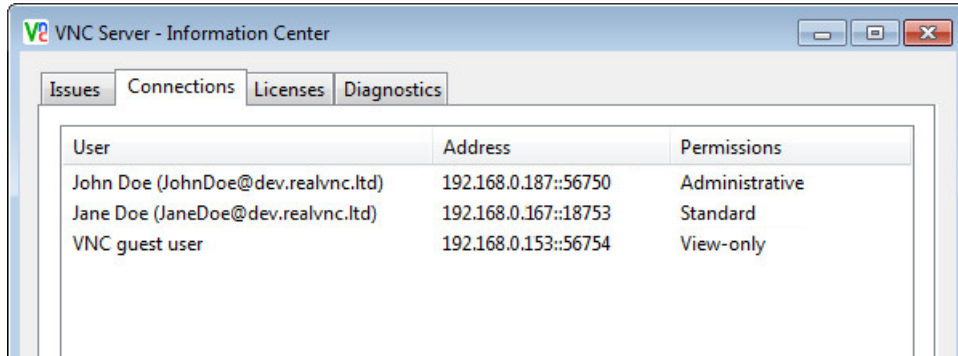
When a user connects to *VNC Server* for the first time, they are asked to verify its identity. For more information on this security feature, see *Verifying the identity of VNC Server on page 115*.

Identifying connected users

The connection bar confirms the number of currently connected users (this bar is only shown if users are actually connected):



Click the **Details** button to identify and manage connected users. The **Connections** tab of the **Information Center** dialog opens (??tab order changed?):



In this example, the user of client computer 192.168.0.187:

- Authenticated to *VNC Server* by supplying the credentials of the John Doe user account. For more information on system authentication, start with *Authenticating using system credentials on page 96*.
- Has an administrative set of VNC permissions, permitting unrestricted access to remote control features while the connection is in progress. For more information, see *Restricting functionality for particular connected users on page 112*.

Click the **Disconnect** button to disconnect a selected user.

Showing expiry dates

The **Details** section reveals expiry dates for *VNC Server* with an Enterprise or a Personal license:

- If you are trialling *VNC Server*, you are informed when your trial expires.
- If you have purchased *VNC Server*, you are informed when your support and upgrades contract expires.

Troubleshooting VNC Server

The **VNC Server** dialog has a colored bar indicating status. *More on this dialog.*

The status bar is green if *VNC Server* is configured correctly:



Note there may be messages to read:



A message indicates that, while *VNC Server* is configured correctly, some minor aspect could be improved.

The status bar turns amber if there are warnings:



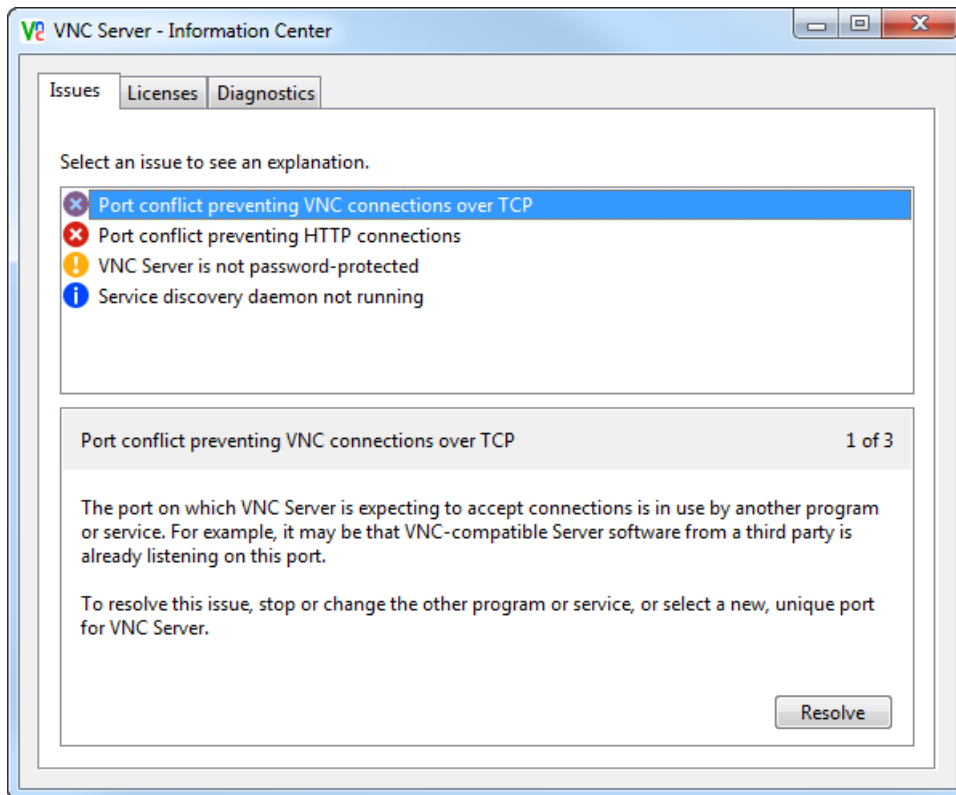
A warning does not prevent users connecting, but indicates that some important aspect of *VNC Server*, such as performance or security, could be improved.

The status bar turns red if there are errors:



An error must be fixed before users can connect.

Click the **Show** button to open the **Information Center** dialog (??tab order changed?):



You can:

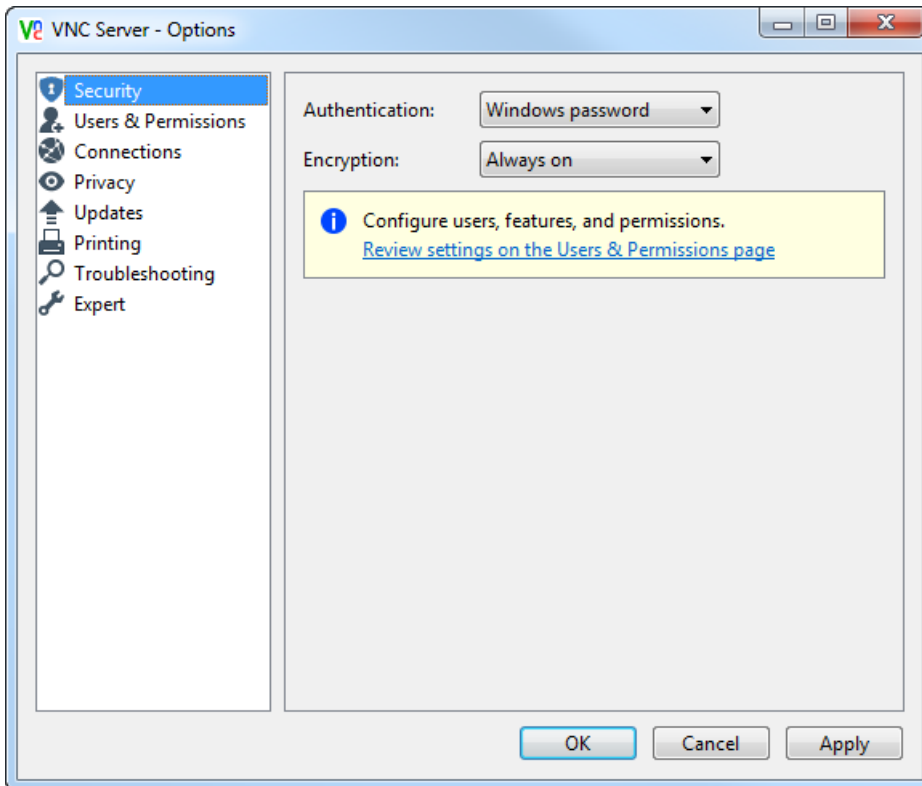
- Repair *VNC Server*. On the **Issues** tab, follow the instructions for each issue.
- List all license keys applied to *VNC Server*, and the features provided by each, on the **Licenses** tab.
- Send system diagnostics to Technical Support. On the **Diagnostics** tab, click the **Save As** button.

- Find out the address of a router protecting the host computer in preparation for Internet connections. On the **Diagnostics** tab, click the **Test Internet Connection** button. See *Connecting over the Internet* on page 28 for more information.

Note: The **Information Center** dialog is also available from the *VNC Server* shortcut menu. *More on this menu.*

Configuring VNC Server

You can configure *VNC Server* once it has started using the **Options** dialog:



Note: To see how to configure *VNC Server* before it starts, or lock down the application to prevent changes, start with *Configuring VNC* on page 130.

To open the **Options** dialog, select **Options** from the *VNC Server* shortcut menu. *More on this menu.* Note that for *VNC Server* in Service Mode, elevated privileges are required.

For information on some of the options in this dialog, see the subsequent sections in this chapter, starting with *Changing ports* on page 90. For security-related information, see *Chapter 7, Making Connections Secure* on page 95. For the **Expert** page, visit www.realvnc.com/products/vnc/documentation/latest/parameters/.

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.

Changing ports

By default, *VNC Server* listens for VNC connection requests on a particular port. In addition, *VNC Server* with an Enterprise or a Personal license listens for *VNC Viewer for Java* download requests on a different port. You can change these ports, or make them the same.

Note: *VNC Viewer for Java* cannot be downloaded from *VNC Server* with a Free license. Upgrade to an Enterprise or a Personal license if flexibility is important to you.

By default, two separate ports are assigned when *VNC Server* starts, one for VNC connections and one for *VNC Viewer for Java* downloads:

- *VNC Server* in both Service Mode and User Mode is assigned port 5900 for connections and port 5800 for downloads.
- Under UNIX, the first instance of *VNC Server* in Virtual Mode is assigned port 5901 for connections and port 5801 for downloads. 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 of *VNC Server*, and the different modes, see *Running VNC Server on page 78*.

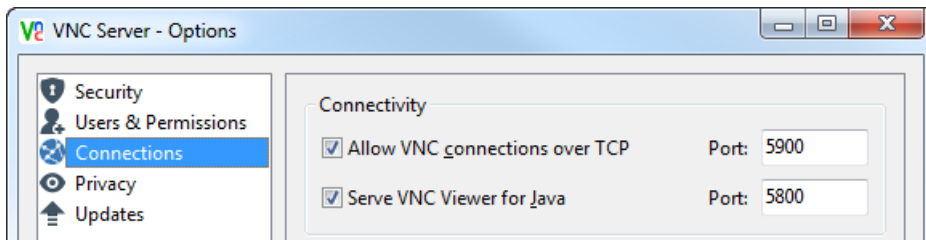
If more than one instance of *VNC Server* is running on a host computer, they must all listen on different ports; see below for information on resolving port conflicts. Note, however, that a particular instance of *VNC Server* can listen on the same port for VNC connections and for *VNC Viewer for Java* download requests; see *Making the connection and download port the same on page 91* 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 VNC connections on port 5900 only. For more information, see *Qualifying a network address with a port number on page 30*.

Resolving port conflicts

VNC Server must listen for VNC connections and *VNC Viewer for Java* download requests on a unique port. This is one on which no other instance of *VNC Server*, nor any other program or service, is listening.

Port conflicts disable *VNC Server*. You should be able to resolve them by changing ports on the **Connections** page of the **Options** dialog. *More on this dialog*.



Changing the connection port

You can change the port on which *VNC Server* is listening for VNC connections. 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 30*.
- 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 31*.
- If the host computer is protected by a router and users are connecting 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 29*.

To change the port, enter a different number in the **Port** field opposite **Allow VNC connections**. 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 30*.
- 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 31*.
- 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 29*.

To change the port, enter a different number in the **Port** field opposite **Serve VNC Viewer for Java**. Note that changing these options does not affect currently connected users.

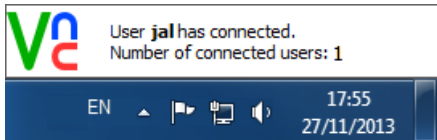
Making the connection and download port the same

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 both **Port** fields. Note that changing these options does not affect currently connected users.

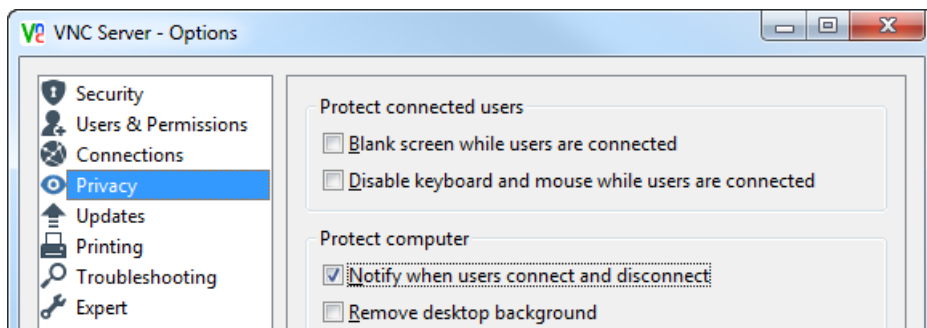
Notifying when users connect

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 user connects:



Note: A similar message appears on disconnection.

You can disable notification messages by turning off **Notify when users connect and disconnect** on the **Privacy** page of the **Options** dialog. *More on this dialog.*



Note: You can replace notifications with connection prompts that enable a host computer (or an already-connected user) to accept or reject new users. For more information, see *Preventing particular users connecting on page 109*.

Stopping VNC Server

VNC Server runs until it is stopped.

To explicitly stop VNC Server in:

- All modes and under all platforms except those below, select **Stop VNC Server** from the VNC Server shortcut menu. *More on this menu.* Administrative privileges may be required.
Note: Under Windows, VNC Server in Service Mode will *not* automatically restart if you do this and then reboot the host computer.
- Service Mode under UNIX, run the appropriate command for your system, for example `/etc/init.d/vncserver-x11-serviced stop` or `systemctl stop vncserver-x11-serviced.service`. For more information, or to see how to prevent VNC Server starting again when the computer is rebooted, visit www.realvnc.com/products/vnc/documentation/latest/reference/vncserver-x11-serviced.html.
- Virtual Mode under UNIX, run the command `vncserver-virtual -kill :x`, where `x` is the X Window System display number. For more information, see *Connecting to VNC Server in Virtual Mode on page 80*.

Note that VNC Server automatically stops in:

- All modes and under all platforms, when the host computer is powered down.
- User Mode under all platforms, when the user account in which it was started is logged 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 user disconnects** option is changed to `Log the current user account off`. For more information, see *Protecting privacy on page 116*.
- A connected user can explicitly stop VNC Server in User or Virtual Mode.
- A connected user can explicitly stop VNC Server in Service Mode if they have administrative privileges.
- A connected user can log off and/or power down the host computer.

To see how to start VNC Server again, read *Starting VNC Server on page 75*.

7

Making Connections Secure

VNC Server with an Enterprise or a Personal license authenticates connecting users and encrypts connections end-to-end out-of-the-box. This chapter explains how to configure VNC Server to relax the authentication and encryption rules if you consider it safe to do so. Conversely, you can tighten the encryption rules for VNC Server with an Enterprise license, if necessary.

Note: VNC Server with a Free license can authenticate users but not encrypt connections. Upgrade to an Enterprise or a Personal license if security is important to you.

This chapter also explains how to protect the host computer from accidental or malicious damage by users, either by restricting their access to remote control features while connections are in progress, or by preventing them connecting in the first place.

Contents

Authenticating users	96
Authenticating using system credentials	96
Authenticating using a password specific to VNC	98
Relaxing the authentication rules	100
Bypassing the authentication rules	102
Changing the encryption rules	105
Preventing connections to VNC Server	106
Restricting functionality for connected users	110
Verifying the identity of VNC Server	115
Protecting privacy	116

Authenticating users

By default, all connecting users must authenticate to *VNC Server*. Note this is *not* the same as logging on to a user account on the host computer, though the same credentials may be used for both operations.

By default, *VNC Server* with:

- An Enterprise or a Personal license is set to use the system authentication scheme. This means that connecting users can supply the same credentials they use to *log on* to the host computer in order to authenticate to *VNC Server*. Note that user accounts must be *registered* with *VNC Server*. See *Authenticating using system credentials* on page 96.
- A Free license is set to use the VNC authentication scheme. This means that connecting users must supply a password specific to VNC. See *Authenticating using a password specific to VNC* on page 98.

If you consider it safe to do so, you can:

- Relax the authentication rules for all connecting users. See *Relaxing the authentication rules* on page 100.
- Allow *particular* users to bypass authentication. See *Bypassing the authentication rules* on page 102.

Authenticating using system credentials

By default, *VNC Server* with an Enterprise or a Personal license is set to use the system authentication scheme, which means that *VNC Server* is integrated into the credentialing mechanism of the system (whether local, domain, or cloud). This scheme is typically both secure and convenient; system administrators commonly force the adoption of complex user names and passwords in enterprise environments, and users with their own accounts can authenticate using already-familiar credentials.

Note: *VNC Server* with a Free license does not support system authentication. Upgrade to an Enterprise or a Personal license if security is important to you.

To authenticate to *VNC Server*, a connecting user can supply the credentials:

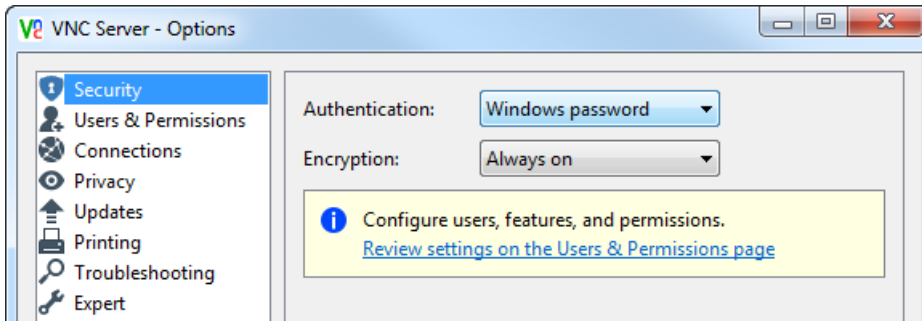
- Under any platform, of a local user account (that is, one set up directly on the host computer).
- Under Windows and Mac OS X, providing the host computer is joined to a domain, of a domain user account (one that is managed by a network service such as Active Directory). Note that prior configuration is required to use domain accounts under UNIX; see *Managing system authentication* on page 141 for more information.
- Under Windows 8, providing the host computer is connected to the Internet, of a cloud user account (that is, a “Microsoft account,” in which the email address constitutes the user name).

Certain user accounts and groups are pre-registered with *VNC Server*, to enable basic connectivity out-of-the-box. See *Managing the list of registered user accounts and groups* on page 97 for more information.

Note: Under Windows, it is possible to create a local user account for a computer that does not have a password set (this is likely for friends and family only). However, a connecting user cannot leave the *VNC Viewer* **Password** field empty. Either change the authentication scheme, or specify a password for the local user account (recommended).

Note that under any platform, the credentials supplied by a user in order to authenticate to *VNC Server* determine the VNC permissions granted to that user. VNC permissions control the availability of remote control features such as file and chat while their connection is in progress. By default, an administrative set of VNC permissions is granted. For more information on what this means, and to see how to revoke VNC permissions in order to disable remote control features, see *Restricting functionality for particular connected users* on page 112.

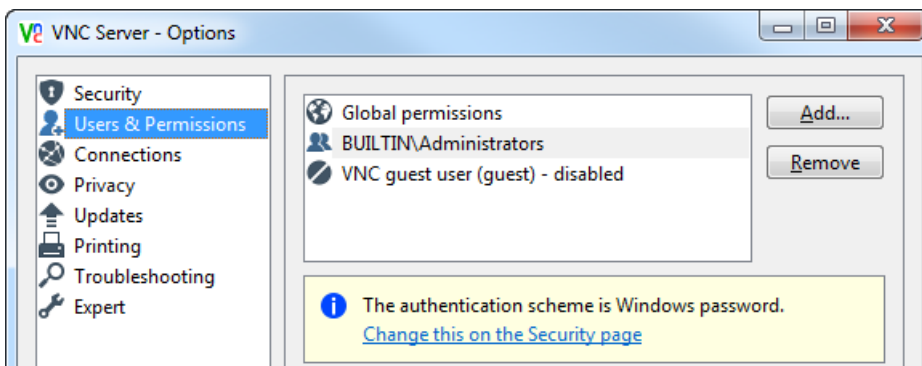
Under each platform, system authentication is managed by an appropriately-named option in the **Security > Authentication** dropdown of the **Options** dialog. *More on this dialog.*



Note: This option is called `UNIX password` and `Mac password` under their respective platforms.

Managing the list of registered user accounts and groups

User accounts must be *registered* with *VNC Server* in order that connecting users may authenticate using familiar, securely-managed system credentials. To see which user accounts and groups are currently registered, ensure system authentication is selected in the **Security > Authentication** dropdown of the **Options** dialog, and open the **Users & Permissions** page:



(VNC Server in Service Mode under Windows)

In this example, the built-in Windows `Administrators` group is registered, which means that any user in this group can authenticate to *VNC Server*. Note this group typically includes Domain Admins if the host computer is joined to a domain.

Note: Guest access is disabled by default. See *Allowing a Guest to connect* on page 103 for more information.

The following table lists the pre-registered user accounts and groups for all platforms and modes, to enable connectivity out-of-the-box:

Mode	Windows	Mac OS X	UNIX
Service	Administrators group	admin group	<ul style="list-style-type: none"> • root user account • admin group • sudo group (Linux only)
User	User account starting <i>VNC Server</i>	User account starting <i>VNC Server</i>	User account starting <i>VNC Server</i>
Virtual	—	—	User account starting <i>VNC Server</i>
Virtual Daemon	—	—	Any user account on the system, including domain accounts if joined to a domain.

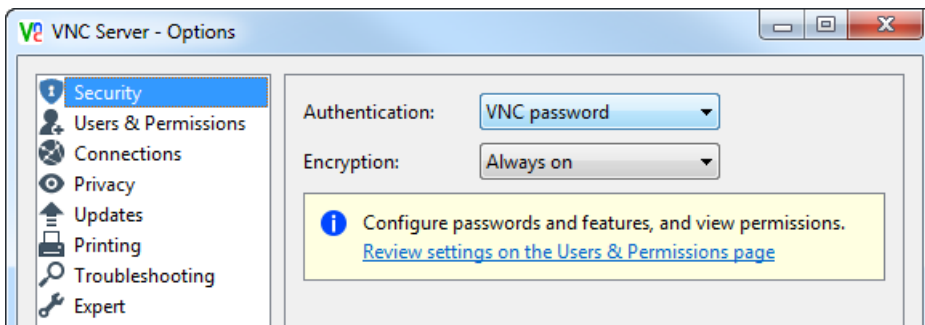
To add a new user account or group, click the **Add** button, and follow the instructions. Note if you remove all user accounts and groups from the list, connections cannot be established.

Authenticating using a password specific to VNC

By default, *VNC Server* with a Free license is set to use the VNC authentication scheme, which means that *VNC Server* has its own password, disassociated from the credentialing mechanism of the system. Note this scheme is only as secure as the complexity of the password chosen.

Note: You can specify VNC authentication for *VNC Server* with an Enterprise or a Personal license if you wish.

VNC authentication is managed by the `VNC password` option in the **Security > Authentication** dropdown of the **Options** dialog. *More on this dialog.*



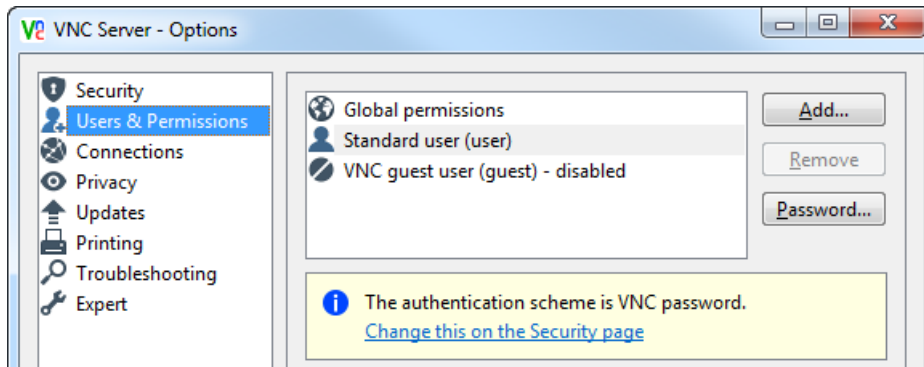
To specify a new or to change an existing password, open the **Users & Permissions** page, select the **Standard** user, and click the **Password** button. Note that connecting users must supply this password in order to authenticate to *VNC Server*, but need not provide a user name.

Specifying additional users

If you choose the VNC authentication scheme for *VNC Server* with an Enterprise or a Personal license, you can specify up to two additional users, enabling you to distinguish between view-only, normal, and administrative connections.

Note: *VNC Server* with a Free license does not support additional users. Upgrade to an Enterprise or a Personal license if flexibility is important to you.

To do this, make sure `VNC password` is selected in the **Security > Authentication** dropdown, and open the **Users & Permissions** page:



Note: Guest access is disabled by default. See *Allowing a Guest to connect* on page 103 for more information.

Click the **Add** button, and follow the instructions to create:

- An administrative user. Connecting users must supply the user name `Admin` and the password you specify in order to authenticate to *VNC Server*. These users can bypass connection prompts and, once connected, can use all available remote control features. For more information on connection prompts, see *Preventing particular users connecting* on page 109.
- A view-only user. Connecting users must supply the user name `ViewOnly` and the password you specify in order to authenticate to *VNC Server*. Once connected, users can observe but not interact.

Relaxing the authentication rules

By default, the most secure authentication scheme available for your license is chosen for *VNC Server*. See *Authenticating users* on page 96 for more information.

The following table explains ways in which you can relax the authentication rules for all prospective users if you consider it safe to do so.

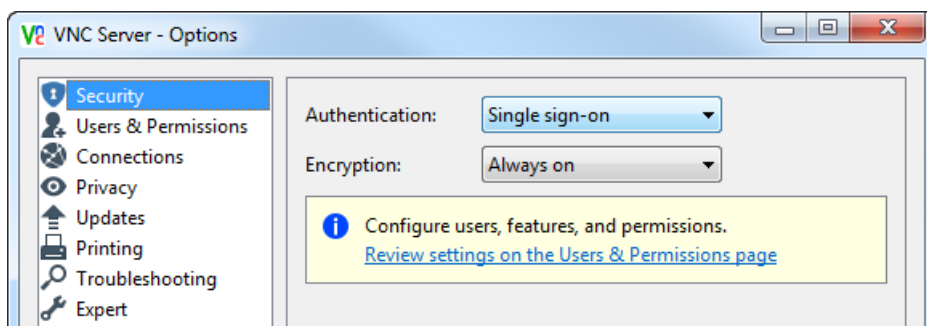
	VNC Server		
	Enterprise	Personal	Free
Authenticate users without interaction. See <i>Authenticating users automatically</i> on page 100.	YES	—	—
Require connecting users to supply just a password. See <i>Authenticating using a password specific to VNC</i> on page 98.	YES	YES	(default)
Disable authentication. See <i>Turning authentication off</i> on page 101.	YES	YES	YES

Authenticating users automatically

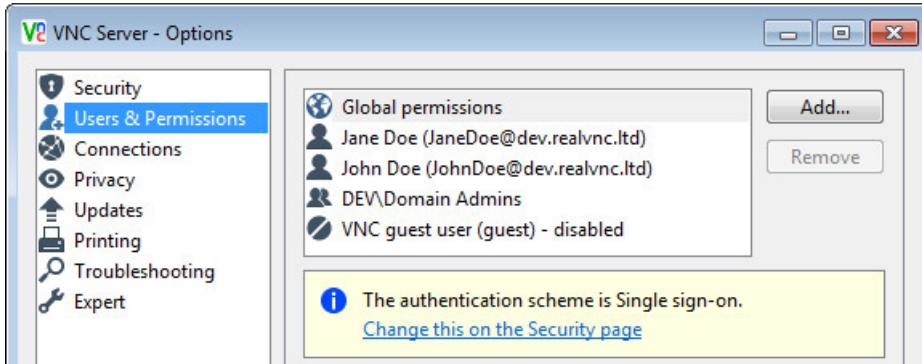
For *VNC Server* with an Enterprise license, you can specify the single sign-on (SSO) authentication scheme. This means that system credentials already entered by connecting users in order to log on to some other system service (perhaps their client computers) are automatically used to authenticate to *VNC Server*. Note this is only possible in a managed network environment; see *Setting up single sign-on authentication* on page 142 for more information.

Note: Single sign-on authentication is not available for *VNC Server* with a Personal or a Free license. Upgrade to an Enterprise license if flexibility is important to you.

To do this, choose the *Single sign-on* option from the **Security > Authentication** dropdown of the **Options** dialog. *More on this dialog.*



Note that the domain accounts of all prospective users must be registered with VNC Server on the **Users & Permissions** page:



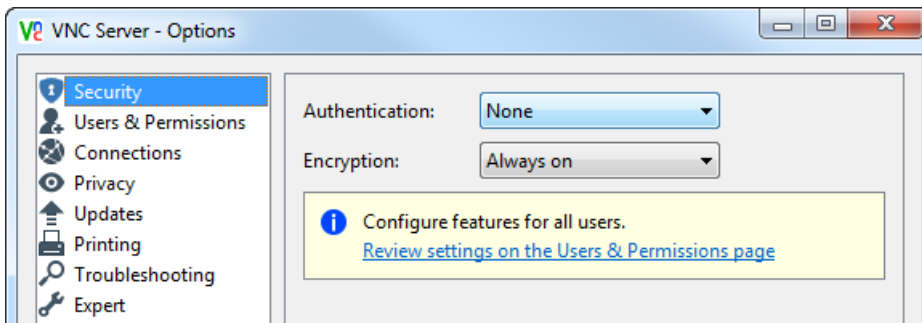
See *Managing the list of registered user accounts and groups* on page 97 for more information. Note that VNC permissions are granted to each connected user in the same way as for system authentication.

Turning authentication off

You can turn authentication off if you are sure all prospective users are trustworthy.

Note: Alternatively, you can allow just *particular* users to bypass authentication. See *Bypassing the authentication rules* on page 102 for more information.

To do this, choose the **None** option in the **Security > Authentication** dropdown of the **Options** dialog. *More on this dialog.*



Bypassing the authentication rules

You can allow just *particular* users to bypass the authentication scheme, keeping VNC Server password-protected.

Note: You can turn authentication off for all users if you consider it safe to do so. See *Turning authentication off* on page 101.

You can:

- Establish a reverse connection to a particular client computer. See *Establishing a reverse connection* on page 102.
- If VNC Server has an Enterprise or a Personal license, allow a particular user to connect as a Guest. See *Allowing a Guest to connect* on page 103.

Clearly, you should only establish reverse connections to client computers with trustworthy prospective users, and only allow trustworthy users to connect as Guests.

Note: If you are setting up VNC Server for unattended access, note that a host computer user must be present for either of these features to work.

Establishing a reverse connection

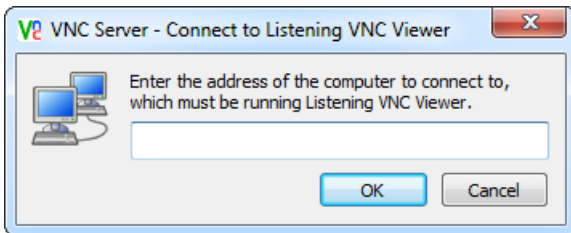
You may be able to establish a reverse connection to a particular client computer, allowing the user of that computer to bypass the authentication scheme.

Note: The client computer must be running *Listening VNC Viewer*. For more information, see *Starting Listening VNC Viewer* on page 36.

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

To establish a reverse connection from the user interface (visit www.realvnc.com/products/vnc/documentation/latest/reference/vncserver-operations.html for command line instructions):

1. Open the VNC Server shortcut menu. *More on this menu.*
2. Select **Connect to Listening VNC Viewer**:



3. If you are connecting:

- Within a private network, enter the network address of the client computer itself. If you do not know what this is, 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 what this is, 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 28.

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 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 26.

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, start with *Chapter 3, Using VNC Viewer* on page 35.

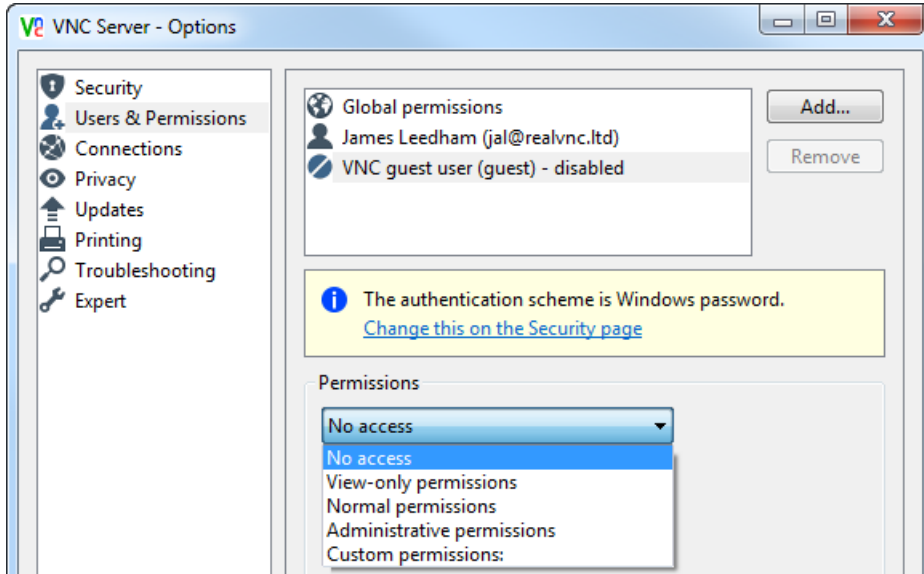
Allowing a Guest to connect

If *VNC Server* has an Enterprise or a Personal license, you can allow a particular user to connect as a Guest, bypassing the authentication scheme. A Guest typically connects infrequently, or for a short period of time.

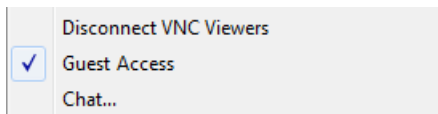
Note: This feature is not available for *VNC Server* with a Free license. Upgrade to an Enterprise or a Personal license if flexibility is important to you.

To enable Guest access:

1. On the **Users & Permissions** page of the **Options** dialog, select VNC guest user. *More on this dialog.* (??swap out James Leedham for John Doe?)



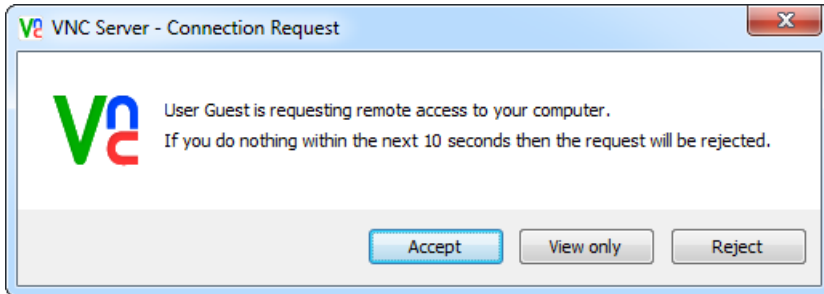
2. In the **Permissions** area, change No access to:
 - View-only permissions to allow connected Guests to observe but not interact.
 - Normal permissions to allow connected Guests to use all remote control features.
 - Administrative permissions to allow connecting Guests to bypass connection prompts, and then use all remote control features.
 - Custom permissions to customize access; see page 113 for more information.
3. On the VNC Server shortcut menu, turn on **Guest Access**. *More on this menu.* A tick appears:



Note: If the **Guest Access** menu option is turned off, guests cannot connect. Note that other connected users can turn this menu option on and off.

Connecting users must supply the user name `Guest`. There is no need to supply a password.

Unless you grant `Administrative` permissions to Guests, each is subject to a connection prompt, giving the host computer (or an already-connected) user the ability to accept or reject the connection, or make it view-only:



By default, if no response is received within ten seconds, the connection is automatically rejected. For more information on connection prompts, see *Preventing particular users connecting* on page 109.

Changing the encryption rules

By default, connections to *VNC Server* with an Enterprise or a Personal license are encrypted end-to-end using 128-bit AES technology.

Note: Connections to *VNC Server* with a Free license cannot be encrypted. Upgrade to an Enterprise or a Personal license if security is important to you.

For *VNC Server* with an Enterprise license, you can:

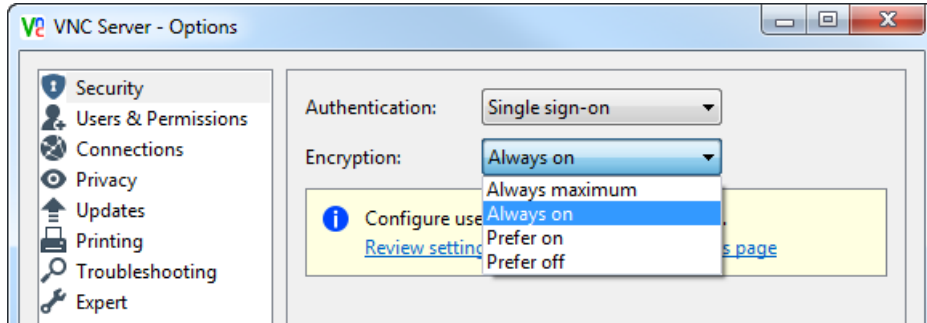
- Relax the encryption rules if you are sure all potential client computers are within a secure network environment, and that eavesdropping is impossible. This may improve performance. It may also allow older versions of *VNC Viewer*, or VNC-compatible Viewer technology, that do not support encryption to connect.

Note: Even if encryption is turned off, a password supplied by a connecting user in order to authenticate to *VNC Server* is always encrypted.

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

For *VNC Server* with a Personal license, you can only relax the encryption rules; 256-bit AES encryption is not available. Upgrade to an Enterprise license if maximum security is important to you.

To change the encryption rules, select an alternative to the default `Always on` option from the **Security > Encryption** dropdown of the **Options** dialog. *More on this dialog.*



Choose:

- `Always maximum` to specify 256-bit AES. Note that only *VNC Viewer 4.6* or later can connect. A connecting user cannot request that encryption be turned off, or the AES key size be reduced to 128-bit.
- `Prefer on` to prefer, though not mandate, that connections be encrypted using 128-bit AES. A connecting user can request either that encryption be turned off (by selecting `Prefer off` in the **VNC Viewer** dialog), or the AES key size be increased to 256-bit (by selecting `Always maximum` in the **VNC Viewer** dialog).
- `Prefer off` to prefer, though not mandate, that connections be unencrypted. 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 to 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 encrypted connection* on page 22.

Preventing connections to VNC Server

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

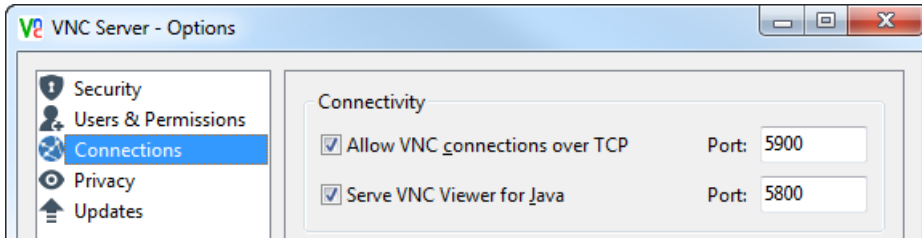
- Users can connect to *VNC Server*.
- If *VNC Server* has an Enterprise or a Personal license, web browser users can download *VNC Viewer for Java* and use it to connect.

You can:

- Prevent all incoming connections (reverse connections can still be established). See *Preventing all incoming connections* on page 107.
- Prevent connections from *particular* client computers. See *Preventing connections from particular client computers* on page 107.
- Prevent *particular* users connecting. See *Preventing particular users connecting* on page 109.

Preventing all incoming connections

You can prevent all incoming connections on the **Connections** page of the **Options** dialog. *More on this dialog.*



To:

- Prevent all incoming connections, including *VNC Viewer for Java* downloads, turn off **Allow VNC connections over TCP**.
- Prevent just *VNC Viewer for Java* downloads, turn off **Serve VNC Viewer for Java**.

Note that:

- Currently connected users are not affected.
- You can still use *VNC Server* to establish reverse connections to client computers. See *Establishing a reverse connection* on page 102 for more information.

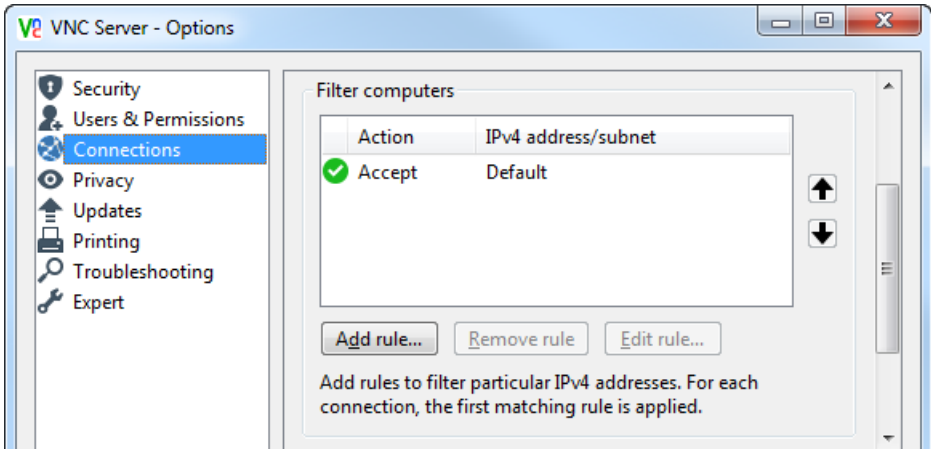
Preventing connections from particular client computers

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

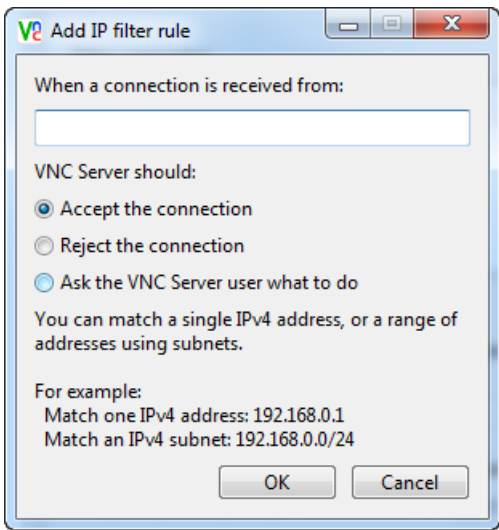
Note: If you filter computers, users can no longer supply IPv6 network addresses in order to connect to *VNC Server* (even from authorized client computers). This is a known restriction.

By default, connections are accepted from all client computers. To filter one or more computers:

1. Open the **Connections** page of the **Options** dialog. *More on this dialog.*



2. Click the **Add rule** button:



3. Specify a IPv4 network address, or range of addresses, and then choose one of the following options:

To:	Choose:
Accept connections from matching client computer(s).	Accept the connection
Reject connections from matching client computer(s).	Reject the connection

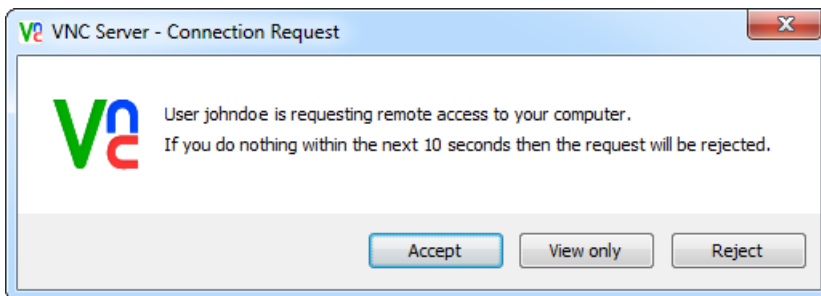
To:	Choose:
Subject connections from matching client computer(s) to connection prompts, giving the host computer (or an already-connected) user the ability to accept or reject each connection, or make it view-only. For more information on connection prompts, see <i>Preventing particular users connecting</i> on page 109.	Ask the VNC Server user what to do

Note that if you create multiple filter rules, their order in the list on the **Connections** page is important. The first matching rule determines what happens to a particular client computer. For example, if a rule rejecting a client computer is encountered before one accepting it, then all connections from that client computer will be rejected. You can move rules up and down in the list using the arrows.

By default, the `Default` rule *accepts* connections from all client computers. You can change this so that it rejects or queries all connections instead. To do this, select the `Default` rule, and click the **Edit rule** button. Note this rule is always last in the list.

Preventing particular users connecting

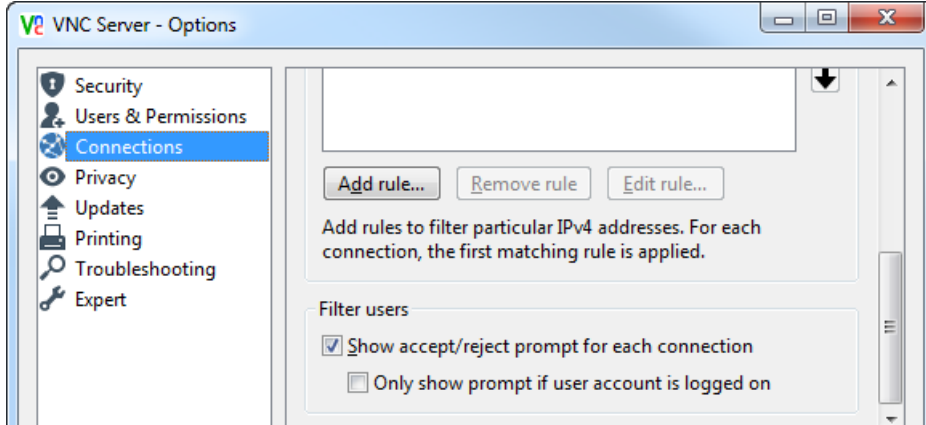
You can prevent a particular user connecting by causing connection prompts to appear on the host computer's desktop:



A connection prompts enables a host computer (or an already-connected) user to identify a connecting user and either accept or reject their connection, or make it view-only. By default, if no response is received within ten seconds, the connection is automatically rejected. Note if you are setting up *VNC Server* for unattended access then enabling this feature may prevent users connecting.

Note: In some circumstances, certain users are able to bypass connection prompts. To see how to subject these users to prompts, read *Restricting functionality for particular connected users* on page 112.

To show connection prompts, turn on **Show accept/reject prompt for each connection** on the **Connections** page of the **Options** dialog. *More on this dialog.*



Note: This option has a slightly different name under *VNC Server* in Virtual Mode.

Restricting functionality for connected users

By default, any number of users can connect to *VNC Server*, and immediately:

- Control the host computer using their keyboard.
- Control the host computer using their mouse.
- Copy and paste text between applications running on the host and their client computer.

If *VNC Server* has an Enterprise or a Personal license, connected users can also:

- Chat with other users connected to the same host computer, or with a host computer user.
- files in either direction.
- Print to a local printer (that is, one connected to the client computer).

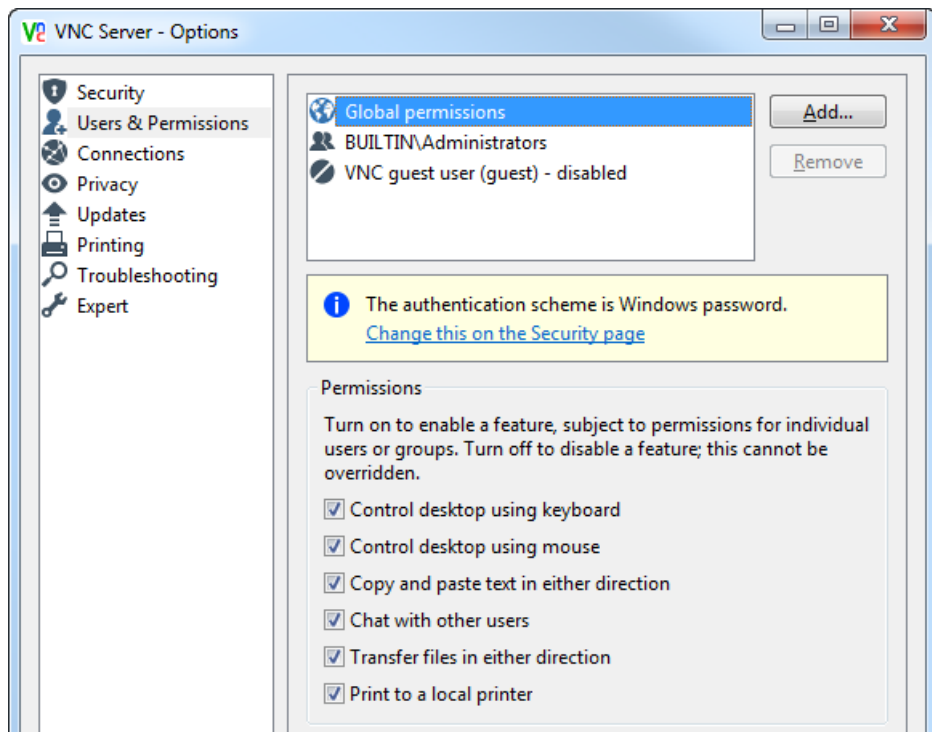
You can:

- Restrict functionality for all connected users. See *Restricting functionality for all connected users* on page 111.
- For *VNC Server* with an Enterprise or a Personal license, restrict functionality for *particular* connected users. See *Restricting functionality for particular connected users* on page 112.

Restricting functionality for all connected users

You can restrict access to remote control features for all connected users, if necessary, by disabling features.

To do this, open the **Users & Permissions** page of the **Options** dialog. *More on this dialog.* Select **Global** permissions, and turn off individual features:



(VNC Server with an Enterprise or a Personal license. A Free license has fewer features.)

Restricting functionality for particular connected users

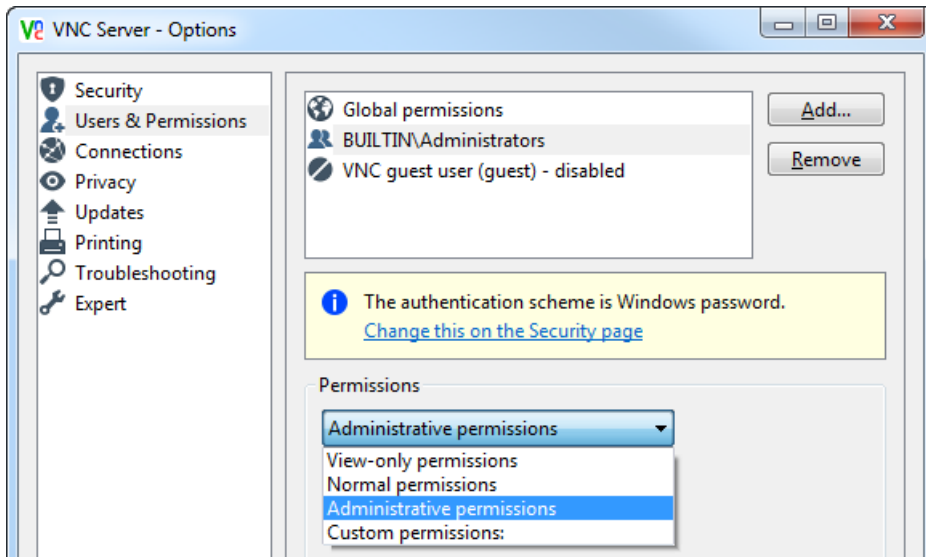
If *VNC Server* has an Enterprise or a Personal license, and the authentication scheme is either:

- System authentication; see *Authenticating using system credentials* on page 96
- Single sign-on; see *Authenticating users automatically* on page 100 (Enterprise licenses only)

then a configurable set of VNC permissions is granted to each user account registered with *VNC Server*, or to all the user accounts in a registered group.

Note: Configurable permissions are not available for the VNC authentication scheme. Choose a different scheme, or upgrade from *VNC Server* with a Free license.

To see the list of registered user accounts and groups, open the **Users & Permissions** page of the **Options** dialog. *More on this dialog.*

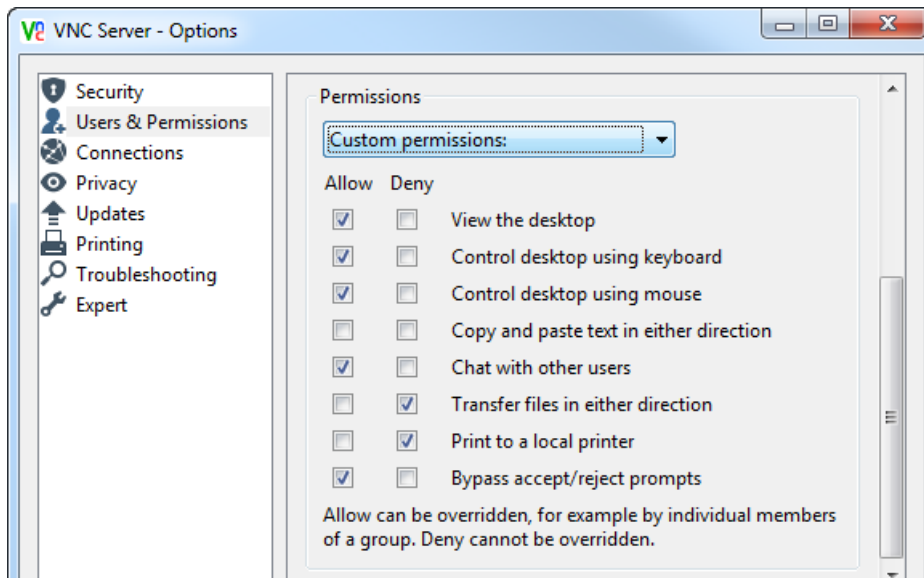


In this example, the built-in Windows Administrators group grants an *administrative* set of permissions to all users in the group. For more information, and to see which user accounts and groups are pre-registered with *VNC Server*, read *Managing the list of registered user accounts and groups* on page 97.

To change the permissions granted by a particular user account or group, select it in the list and, from the **Permissions** dropdown, choose either:

- View-only permissions to allow connected users to observe but not interact.
- Normal permissions to grant connected users access to all remote control features.
- Administrative permissions to allow connecting users to bypass connection prompts, and then grant access to all remote control features.

Alternatively, to tailor permissions more precisely, choose Custom permissions:



To:

- Grant permission to use a particular feature, turn on **Allow**. If a group is selected, this can be overridden for an individual member by turning on **Deny**.
- Disallow permission to use a feature, turn off **Allow**. If a group is selected, this can be overridden for an individual member by turning on **Allow** or **Deny**.
- Disable a feature, turn on **Deny**. This cannot be overridden.

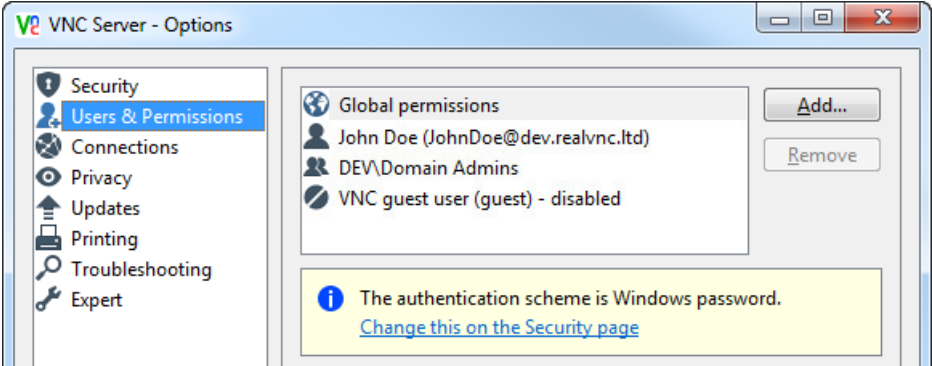
Note that:

- Omitting to grant the View the desktop permission means connected users see only a blank screen.
- Granting permission to use the following features has no effect if those features are disabled globally:

Control desktop using keyboard
 Control desktop using mouse
 Copy and paste text in either direction
 Chat with other users
 files in either direction
 Print to a local printer

See *Restricting functionality for all connected users* on page 111 for more information.

Consider the following example of a registered `Domain Admins` group consisting of two user accounts, `johndoe` and `janedoe`. The `johndoe` user account is also registered separately, for fine-grained control:



The following table explains for whom the printing feature is available given that `johndoe` inherits permissions from `Domain Admins`, but can override these in certain circumstances:

Is printing available?		johndoe		
		<input checked="" type="checkbox"/> Allow	<input type="checkbox"/> Allow	<input checked="" type="checkbox"/> Deny
Domain Admins	<input checked="" type="checkbox"/> Allow	YES	janedoe: YES johndoe: NO	janedoe: YES johndoe: NO
	<input type="checkbox"/> Allow	janedoe: NO johndoe: YES	NO	NO
	<input checked="" type="checkbox"/> Deny	NO	NO	NO

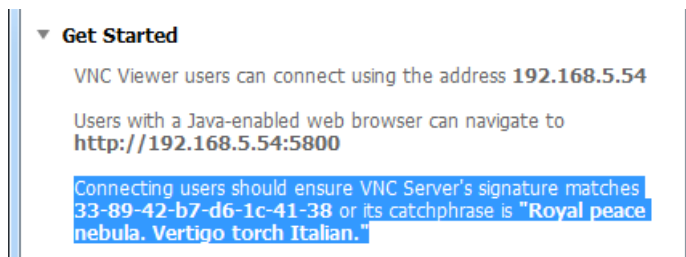
Verifying the identity of VNC Server

VNC Server with an Enterprise or a Personal license has a digital signature:

- Under Windows and Mac OS X, this signature uniquely identifies a particular instance of *VNC Server* running on a host computer.
- Under UNIX, this signature is shared by all instances of *VNC Server* started by the same computer user.

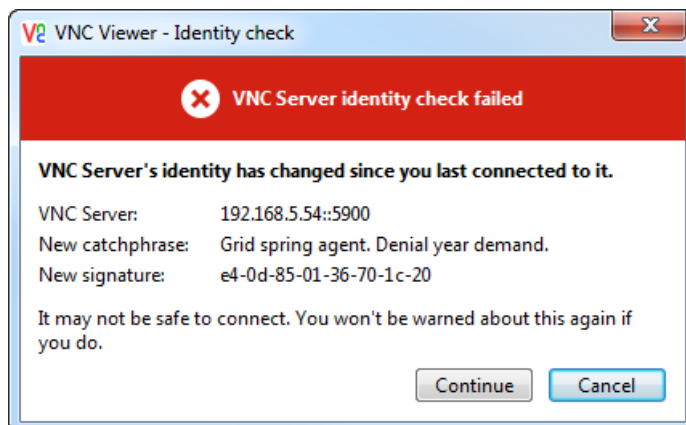
Note: This feature is not available for *VNC Server* with a Free license. Upgrade to an Enterprise or a Personal license if security is important to you.

The *VNC Server* signature and catchphrase (a more-memorable version of the signature) are displayed in the **Get Started** area of the **VNC Server** dialog. *More on this dialog.*



When a user connects from a particular client computer for the first time, the signature and catchphrase are published. The user is asked to verify that the information they see matches that of *VNC Server*; see *Checking the identity of VNC Server* on page 24 for more information.

A *VNC Server* signature should not change. The next (and all subsequent) times a user connects from the same client computer, the signature is *not* published. If the signature changes, it may be because a third party is interrupting the connection between client and host computers and eavesdropping on communications – a so-called ‘man-in-the-middle’ attack. If a user sees a message similar to the following:



then it is recommended that that user does *not* connect.

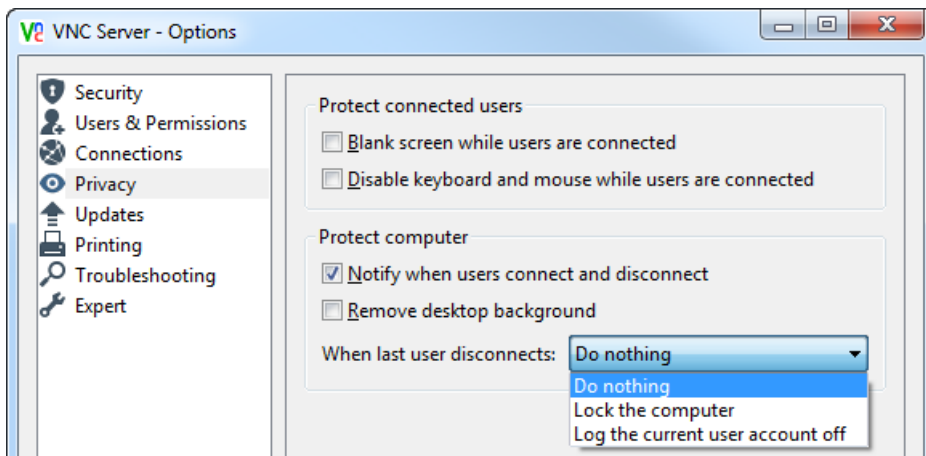
Note: The signature *does* change if *VNC Server* is re-installed, or if the private key is regenerated.

Protecting privacy

By default, *VNC Server* promotes sharing. That is to say, multiple users can connect at the same time, all connected 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.

Note: To allow only one connection at a time, specify *VNC Server* parameters; start with www.realvnc.com/products/vnc/documentation/latest/parameters/vncserver.html#alwaysshared for more information.

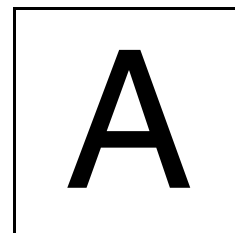
Under some platforms, you can configure *VNC Server* to uphold other aspects on the **Privacy** page of the **Options** dialog. *More on this dialog.*



To:

- Prevent a host computer user observing the operations of connected users, turn on **Blank screen while users are connected** (Windows only; not available under Windows 8).
- Prevent a host computer user interrupting the operations of connected users, turn on **Disable keyboard and mouse while users are connected** (Windows only).
- Protect the host computer when no connections are in progress, select an appropriate option from the **When last user disconnects** dropdown (Windows and Mac OS X 10.5+; *VNC Server* in Service Mode only).

For more information on notification messages, see *Notifying when users connect* on page 92.



Saving Connections

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

Note: You can save connections to desktop icons. You can save connections to *VNC Address Book* if you installed *VNC* on the client computer. See *Setting up the client computer* on page 12 for more information.

A saved connection remembers the network address of the host computer and the authentication credentials required to connect to *VNC Server*, so you do not have to, and automatically recreates your preferred working environment each time.

Contents

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

Saving connections to VNC Address Book

You can save connections to *VNC Address Book* if you installed *VNC* on the client computer. For more information, see *Setting up the client computer* on page 12.

Note: If *VNC Address Book* is not available, you can save connections to desktop icons. This is equally convenient but may be less secure. See *Saving connections to desktop icons* on page 127.


When you save a connection, you can subsequently use *VNC Address Book* to connect to that host computer instead of *VNC Viewer*. This means you do not have to remember the network address of the host computer or the port number for *VNC Server*, nor a user name and password. In addition, *VNC Address Book* automatically recreates the *VNC Viewer* environment you chose for controlling that host computer last time, for example the scaling applied to the desktop, the encryption level, and the color quality.

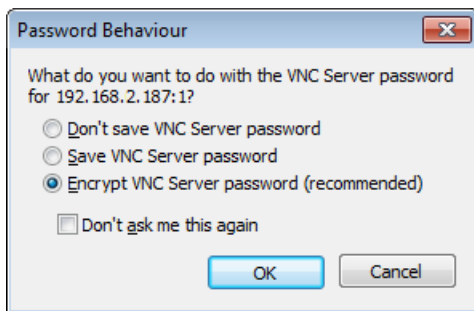
Note: Because *VNC Address Book* stores *VNC Server* authentication credentials, access to it is controlled by a *master password*. For more information, see *Working with the master password* on page 126.

You can additionally 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 connected to a host computer, you can save the current 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:

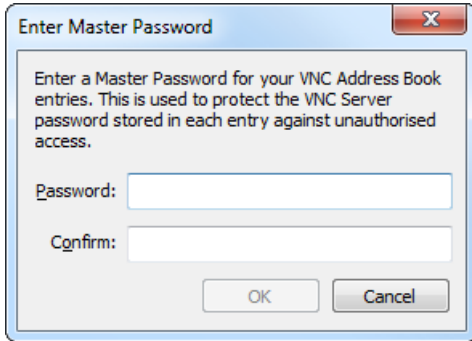


Choose:

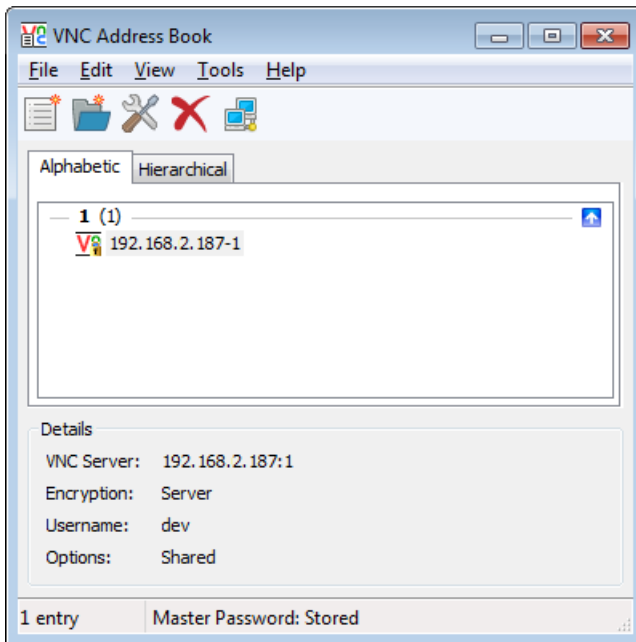
- **Don't save VNC Server password** in order to forget the password. You will need to enter it each time you use *VNC Address Book* to connect.
- **Save VNC Server password** to save the password in obfuscated, though not encrypted, form. You will no longer need to remember the password. However, since 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:



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



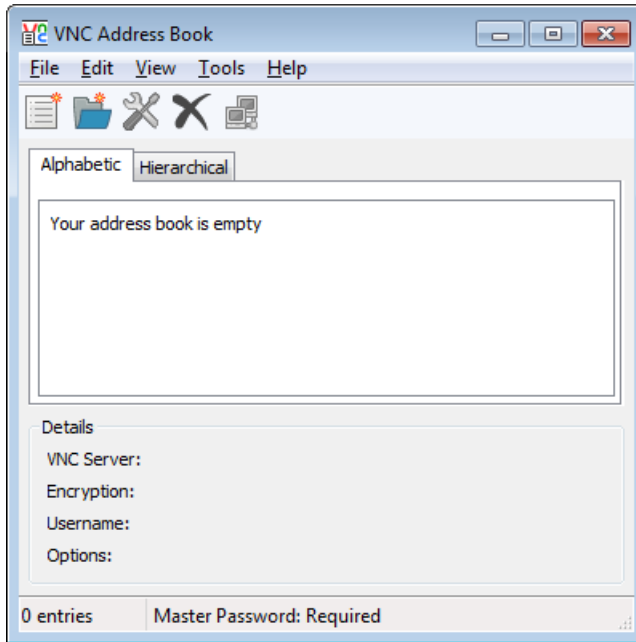
To see how to use VNC Address Book to connect to this host computer again, read *Using VNC Address Book to connect* on page 123.


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

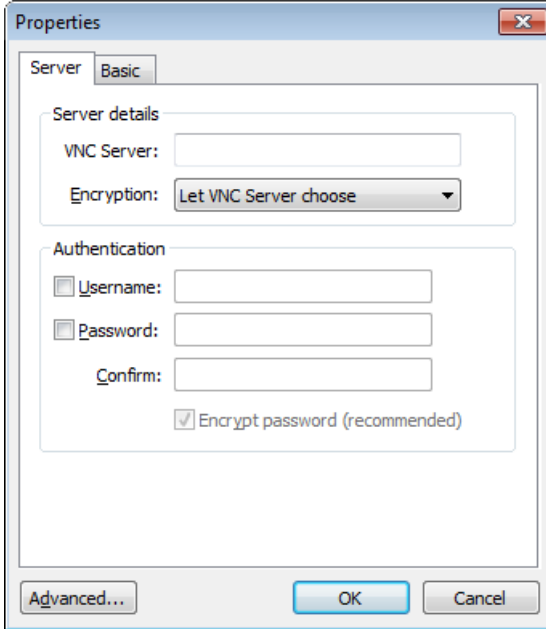
Creating a new connection

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


1. Start *VNC Address Book* on the client computer. See *how to do this*. The **VNC Address Book** dialog opens:



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



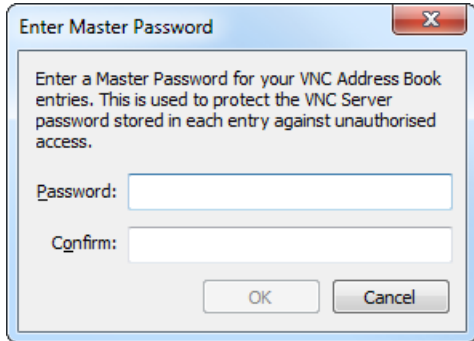
3. Enter a network address for the host computer in the **VNC Server** field (including a port number if necessary), choose an **Encryption** option (or retain the default) and, optionally, specify your VNC Server user name and password in the **Authentication** area. To see how to find out this information, start with *Step 3: Identify VNC Server running on the host computer on page 21*.

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.

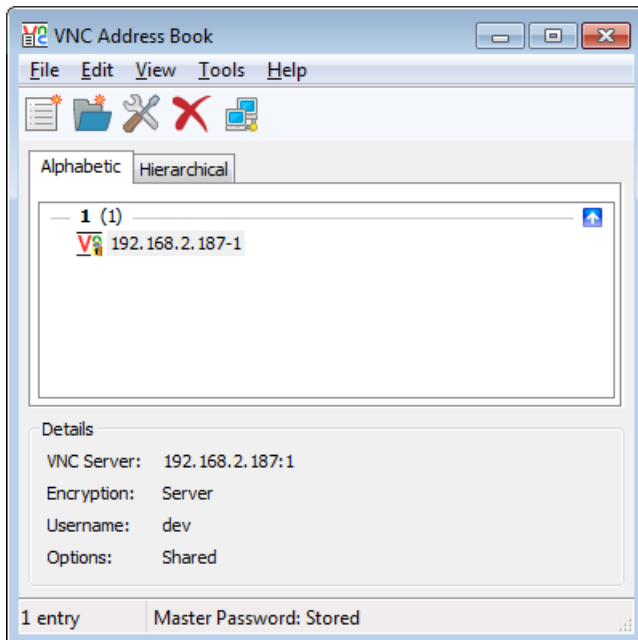
Note: Turn off **Encrypt password (recommended)** if you do not want to enter the VNC Address Book master password in order to connect. Note this may constitute a security risk if others use your client computer.

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 37*.

- 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:



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



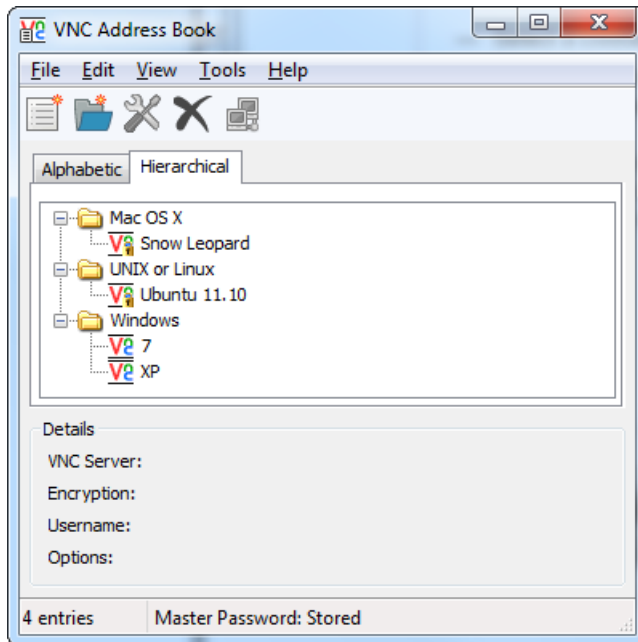
To see how to use *VNC Address Book* to connect to this host computer, read *Using VNC Address Book to connect* on page 123.

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


Using VNC Address Book to connect

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


1. Start *VNC Address Book* on the client computer. See *how to do this*. The **VNC Address Book** dialog opens:



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 126.

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

Managing connections using VNC Address Book



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

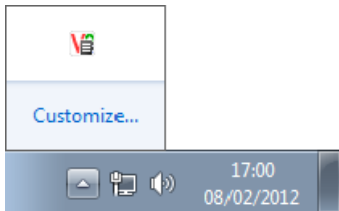
Starting VNC Address Book

To start *VNC Address Book*:

- Under Windows, select **RealVNC > VNC Address Book** from the **Start** menu.
Note: Under Windows, you can start *VNC Address Book* automatically when the computer is powered on. To do this, select **Tools > Options** and, in the **UI behavior** area, turn on **Start with Windows**.
- Under UNIX, select **Applications > Internet > VNC Address Book** from the menu system, or search for this application using the standard operating system facility.
Note: If no menu system or search facility is available, open a Terminal window and run the command `vncaddrbook`. Note you should *not* do this as a user with administrative privileges.
- Under Mac OS X, navigate to **Applications > RealVNC**, and double-click **VNC Address Book**.

Working with VNC Address Book

Under Windows, while *VNC Address Book* is running, a *VNC Address Book* icon  is displayed in the Notification area. Under Windows 7, note this is hidden by default and accessible from  to the right of the Taskbar:

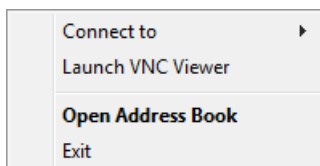


Under Windows XP, the icon may be hidden by other icons.

Note: Under UNIX 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 available, then *VNC Address Book* is not running.
- Has a shortcut menu that performs useful operations:

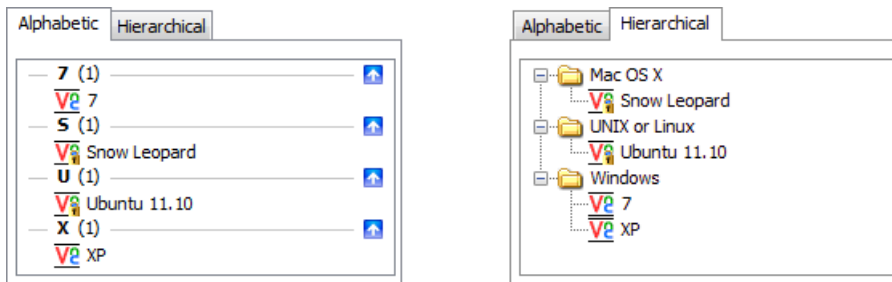


The following table explains the effect of selecting each *VNC Address Book* shortcut menu option.


Option	Purpose
Connect to	Choose a host computer to connect to.
Launch VNC Viewer	Start <i>VNC Viewer</i> , enabling you to connect to a new host computer in the standard way. For more information, see <i>Connecting to a host computer on page 39</i> .
Open Address Book	Create new connections or edit and organize existing ones. (Alternatively, double-click the <i>VNC Address Book</i> icon to open the VNC Address Book dialog.)
Exit	Close <i>VNC Address Book</i> .

Organizing connections

VNC Address Book organizes connections both alphabetically and hierarchically:




You can reorganize connections in the **Hierarchical** list. (The **Alphabetic** 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 **Alphabetic** or **Hierarchical** list, and either:

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

For more information on editing *VNC Viewer* options, start with *Configuring VNC Viewer before you connect on page 37*.

To rename a connection in *VNC Address Book*, select it in the **Alphabetic** 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**  toolbar button.
- Select **Edit > Delete**.

Working with the master password

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

VNC Address Book secures protected connections using the *master password*. You must enter the master password in order to perform an operation on a protected connection, for example connecting to the host computer, or 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 118.

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



You can save the current connection to a desktop icon on the client computer:

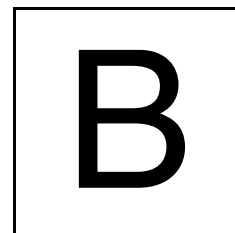


A desktop icon provides an extremely quick and convenient way of connecting to a host computer. Simply double-click the icon to connect. Your preferred *VNC Viewer* environment for controlling the host computer is automatically recreated.

Note: You may need to associate the desktop icon with the *VNC Viewer* executable file the first time you double-click an icon connect.

To save the current connection as a desktop icon:

1. Click the **Save Connection**  *VNC Viewer* toolbar button.
Note: If *VNC Address Book* is installed on the client computer, you must first disable it. 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.



Setting Up VNC

This appendix explains to system administrators how to set up and configure VNC applications for multiple users in an enterprise environment.

Note an Enterprise license for *VNC Server* is required for many features.

Contents

Configuring VNC	130
Specifying VNC parameters	130
Specifying Xvnc options	136
Preventing users configuring VNC	138
Managing system authentication	141
Setting up single sign-on authentication	142
Hosting VNC on a UNIX network share	144
Logging information	147
Completely removing VNC	149

Configuring VNC

VNC applications can be configured in almost any way to suit your requirements and environment.

To configure...	Specify...	
	VNC parameters (page 130)	Xvnc options (page 136)
VNC Server in Virtual Mode under UNIX	YES	YES
All other VNC applications and platforms	YES	—

You can:

- Configure VNC applications on the same computer on which applications are installed; start with *Specifying VNC parameters* on page 130.
- Remotely configure and lock down VNC applications using policy; start with *Preventing users configuring VNC* on page 138.
- Remotely configure VNC applications on Windows computers using *VNC Deployment Tool*; visit www.realvnc.com/products/vnc/deployment/vnctool/.
- Host certain VNC applications on a UNIX network share and specify a single set of preferences centrally; see *Hosting VNC on a UNIX network share* on page 144.

For more information on remote configuration options, start with www.realvnc.com/products/vnc/deployment/.

By default, users can configure VNC applications. To see how to prevent or mitigate against this, see *Preventing users configuring VNC* on page 138.

Specifying VNC parameters

All VNC applications are controlled by VNC parameters, set to suitable default values for most users out-of-the-box.

You can configure any VNC application by specifying new values for VNC parameters:

- Before the application starts. See *Configuring VNC applications before they start* on page 131.
- While the application is running, and connections are in progress. See *Reconfiguring running VNC applications* on page 134.

For explanations of individual parameters, visit www.realvnc.com/products/vnc/documentation/latest/parameters/.

Configuring VNC applications before they start

	Specify VNC parameters...		
To configure VNC applications...	Windows	UNIX	Mac OS X
Prior to start-up	Registry keys (page 131)	VNC configuration files (page 132)	VNC configuration files (page 132)
At start-up (page 134)	Command line (User Mode only)	Command line	Command line
Using policy (page 138)	Registry keys	VNC configuration files	VNC configuration files

Note that parameters are applied in the order listed in the table above, so that a parameter set by policy overrides the same parameter specified at the command line, which in turn overrides the same parameter specified prior to start up. Note that parameters set by policy cannot be changed by users. See the sections below for more information.

Populating the Windows Registry with VNC parameters

Under Windows, if you have permission to edit the Windows Registry, you can specify VNC parameters as values for particular Registry keys.

Note: If you have an Enterprise license, and do not wish to edit the Registry directly, you can set policy or use *VNC Deployment Tool*. Visit www.realvnc.com/products/vnc/deployment/ for more information.

The following table lists the Registry keys to create or edit for each VNC application, and the order in which parameters are applied.

VNC application	Order parameters are applied (lowest takes precedence)	Notes
VNC Server in Service Mode	HKLM\Software\RealVNC\vnserver HKLM\Software\Policies\RealVNC\vnserver	The Options dialog for an application updates a particular Registry key; see <i>this table</i> on page 135. Note it is not possible to specify parameters at the command line for VNC Server in Service Mode.
VNC Server in User Mode	HKCU\Software\RealVNC\vnserver <parameters at the command line> HKCU\Software\Policies\RealVNC\vnserver	
VNC Viewer	HKCU\Software\RealVNC\vnviewer <parameters at the command line> HKCU\Software\Policies\RealVNC\vnviewer	

For example, to specify the `Log` parameter for VNC Server in Service Mode:

1. Using Registry Editor, navigate to `HKEY_LOCAL_MACHINE\Software\RealVNC\vnserver`.
2. Select **New > String Value** from the shortcut menu, and create `Log`.
3. Select **Modify** from the shortcut menu, and specify appropriate **Value data**, for example `*:file:100`.

Note: All VNC parameters take string values, even boolean parameters.

Populating VNC configuration files with VNC parameters

Under UNIX and Mac OS X, each VNC application has a number of VNC configuration files, and additionally a number shared between all VNC applications and user accounts on the computer. The following tables list the files you can create or edit for each application, and the order in which parameters are applied.

UNIX

VNC application	Order parameters are applied (lowest takes precedence)	Notes
VNC Server in User Mode (vncserver-x11)	/etc/vnc/config.d/common.custom /etc/vnc/config.d/vncserver-x11 ~/.vnc/config.d/common ~/.vnc/config.d/vncserver-x11 <parameters at the command line> /etc/vnc/policy.d/common /etc/vnc/policy.d/vncserver-x11	The Options dialog updates a particular VNC configuration file; see <i>this table</i> on page 135. Parameters specified in /etc/vnc/*/vncserver-x11 also affect VNC Server in Service Mode, below.
VNC Server in Service Mode (vncserver-x11, via vncserver-x11-serviced)	/etc/vnc/config.d/common.custom /etc/vnc/config.d/vncserver-x11 /root/.vnc/config.d/common /root/.vnc/config.d/vncserver-x11 /etc/vnc/policy.d/common /etc/vnc/policy.d/vncserver-x11	The Options dialog updates a particular VNC configuration file; see <i>this table</i> on page 135. Parameters specified in /etc/vnc/*/vncserver-x11 also affect VNC Server in User Mode, above.
VNC Server in Virtual Mode (Xvnc, via vncserver-virtual or vncserver)	/etc/vnc/config.d/common.custom /etc/vnc/config.d/Xvnc ~/.vnc/config.d/common ~/.vnc/config.d/Xvnc <parameters at the command line> /etc/vnc/policy.d/common /etc/vnc/policy.d/Xvnc	The Options dialog updates a particular VNC configuration file; see <i>this table</i> on page 135.
VNC Server in Virtual Mode daemon (vncserver-virtuald)	/etc/vnc/config.d/common.custom /etc/vnc/config.d/vncserver-virtuald /root/.vnc/config.d/common /root/.vnc/config.d/vncserver-virtuald <parameters at the command line> /etc/vnc/policy.d/common /etc/vnc/policy.d/vncserver-virtuald	The daemon only accepts a subset of parameters; run <code>vncserver-virtuald -help</code> for a list. The daemon then launches the Xvnc process for each connecting user, at which point its VNC configuration files are applied to it (see VNC Server in Virtual Mode, above). Note this application does not have an Options dialog.
VNC Viewer (vncviewer)	/etc/vnc/config.d/common.custom /etc/vnc/config.d/vncviewer ~/.vnc/config.d/common ~/.vnc/config.d/vncviewer <parameters at the command line> /etc/vnc/policy.d/common /etc/vnc/policy.d/vncviewer	The Options dialog updates a particular VNC configuration file; see <i>this table</i> on page 135.

Mac OS X

VNC application	Order parameters are applied (lowest takes precedence)	Notes
VNC Server in Service Mode	<code>/etc/vnc/config.d/common.custom</code> <code>/etc/vnc/config.d/vncserver</code> <code>/var/root/.vnc/config.d/common</code> <code>/var/root/.vnc/config.d/vncserver</code> <code>/etc/vnc/policy.d/common</code> <code>/etc/vnc/policy.d/vncserver</code>	<p>Parameters specified in <code>/etc/vnc/*.d/vncserver</code> are applied to VNC Server in User Mode too.</p> <p>The Options dialog updates a particular VNC configuration file; see <i>this table</i> on page 135.</p> <p>Note it is not possible to specify parameters at the command line.</p>
VNC Server in User Mode	<code>/etc/vnc/config.d/common.custom</code> <code>/etc/vnc/config.d/vncserver</code> <code>~/.vnc/config.d/common</code> <code>~/.vnc/config.d/vncserver</code> <code><parameters at the command line></code> <code>/etc/vnc/policy.d/common</code> <code>/etc/vnc/policy.d/vncserver</code>	<p>Parameters specified in <code>/etc/vnc/*.d/vncserver</code> are applied to VNC Server in Service Mode too.</p> <p>The Options dialog updates the VNC configuration file in <i>this table</i> on page 135.</p>
VNC Viewer	<code>/etc/vnc/config.d/common.custom</code> <code>/etc/vnc/config.d/vncviewer</code> <code>~/.vnc/config.d/common</code> <code>~/.vnc/config.d/vncviewer</code> <code><parameters at the command line></code> <code>/etc/vnc/policy.d/common</code> <code>/etc/vnc/policy.d/vncviewer</code>	<p>The Options dialog updates the VNC configuration file in <i>this table</i> on page 135.</p>

Sharing VNC configuration files between applications and user accounts

When VNC is installed, `/etc/vnc/config.d/common` is created. This file is reserved for use by RealVNC.

To specify parameters for all VNC applications for all user accounts on the computer, create the following file:

```
/etc/vnc/config.d/common.custom
```

To specify parameters for all VNC applications for a particular user account, create the following file:

```
~/.vnc/config.d/common
```

Note: `~` is the `root` user account for certain applications; see the tables above.

Other VNC configuration files are application-specific. For example, to specify parameters for VNC Server in User Mode for all user accounts on a UNIX computer, create the following file:

```
/etc/vnc/config.d/vncserver-x11
```

To specify parameters for VNC Server in User Mode for a particular user account, create the following file:

```
~/.vnc/config.d/vncserver-x11
```

Note this is the file updated by the **Options** dialog; see *Using the Options dialog* on page 135.

Format of a VNC configuration file

Each parameter in a VNC configuration file should be on a separate line; leading and trailing white space and comments are skipped, and environment variables expanded for parameters that accept them. For example:

```
#This is a comment
Desktop=Build machine
Encryption=AlwaysOn
Authentication=SystemAuth
RsaPrivateKeyFile=$HOME/secure/vnc
Permissions=admin:f,vncusers:d,guests:v
```

Specifying VNC parameters at the command line

Under any platform, for most VNC applications, you can pass VNC parameters in at the command line when you start that application, each preceded by a dash (-). This enables you to configure a particular instance of the application, rather than every time it runs. For example:

```
vncserver-x11 -Desktop="Debug machine" -Authentication=VncAuth
```

Note: You cannot specify parameters at the command line for *VNC Server* in Service Mode. For the *VNC Server* in Virtual Mode daemon, you *can* specify command line parameters in the `/etc/init.d/<daemon>` script or in `/etc/systemd/system/<daemon>.service`, but it is recommended you use VNC configuration files instead.

Parameters specified at the command line override the same parameters specified in the Windows Registry (see *this table* on page 131 for the exact order) or in VNC configuration files (see *these tables* on page 132), except for those set by policy.

Note there are disadvantages to specifying parameters at the command line:

- The **Options** dialog does not reflect your choices, which may confuse users.
- Under UNIX and Mac OS X, parameters may be overridden if a running application is reloaded; see *Reconfiguring running VNC applications* on page 134.

Note: RealVNC recommends specifying parameters *either* in the Windows Registry/VNC configuration files or at the command line, but not both.

For convenience, if you have many command line parameters to specify, you can populate a text file (one parameter per line; omit the dash) and reference it using the `-vncconfigfile` option, for example:

```
vncserver-x11 -vncconfigfile /my/command/line/parameter/file
```

Reconfiguring running VNC applications

You can reconfigure:

- Any VNC application using its **Options** dialog, if it has one; see *Using the Options dialog* on page 135.
- *VNC Server* by reloading parameters; see *Reloading VNC parameters* on page 136.

Note that most changes take effect immediately. Changes to a few parameters, however, require all connections to be terminated, and changes to a very small minority require the application to be restarted. Visit www.realvnc.com/products/vnc/documentation/latest/parameters/ for more information.

Using the Options dialog

Most VNC applications have an **Options** dialog, providing a user-friendly interface to the VNC parameter mechanism. An **Options** dialog typically consists of several tabs or pages devoted to particular topics such as security or connectivity, and an **Expert** tab or page enabling users to edit VNC parameters directly. See a *picture*.

Note the following:

- The **Options** dialog for *VNC Server* in Service Mode requires elevated privileges.
- The **Options** dialog for *VNC Server* in Virtual Mode is only available to *connected* users; see *Working with VNC Server in Virtual Mode* on page 80.
- The **Options** dialog can be hidden from users; see *Mitigating against change* on page 139.
- VNC parameters set by policy are disabled in the **Options** dialog.

Changes made in an **Options** dialog automatically update a particular Registry key or VNC configuration file; see the tables below. When the **OK** or **Apply** button is clicked, *all* Registry keys or VNC configuration files for that application are then reloaded.

Windows

VNC application	The Options dialog updates...
VNC Server in Service Mode	HKLM\Software\RealVNC\vncserver
VNC Server in User Mode	HKCU\Software\RealVNC\vncserver
VNC Viewer	HKCU\Software\RealVNC\vncviewer

See *this table* on page 131 for a complete list of Registry keys and the order in which they are applied.

UNIX

VNC application	The Options dialog updates...
VNC Server in User Mode	~/.vnc/config.d/vncserver-x11
VNC Server in Service Mode	/root/.vnc/config.d/vncserver-x11
VNC Server in Virtual Mode	~/.vnc/config.d/Xvnc
VNC Viewer	~/.vnc/config.d/vncviewer

See *this table* on page 132 for a complete list of VNC configuration files and order in which they are applied.

Mac OS X

VNC application	The Options dialog updates...
VNC Server in Service Mode	/var/root/.vnc/config.d/vncserver
VNC Server in User Mode	~/.vnc/config.d/vncserver
VNC Viewer	~/.vnc/config.d/vncviewer

See *this table* on page 133 for a complete list of VNC configuration files and order in which they are applied.

Reloading VNC parameters

You can reconfigure a running instance of *VNC Server* without downtime by editing Registry keys (Windows) or VNC configuration files (other platforms) and then running the `-reload` command to re-apply *all* Registry keys or VNC configuration files to that instance of *VNC Server*. For example:

```
vncserver-x11 -reload
```

Note that:

- The `-reload` command also re-applies license keys.
- The `-reload` command does *not* re-apply:
 - VNC parameters specified at the command line under UNIX and Mac OS X. If these parameters have subsequently changed, the original command line values will be overridden. See *Specifying VNC parameters at the command line* on page 134 for more information.
 - Xvnc options, for *VNC Server* in Virtual Mode under UNIX. See *Specifying Xvnc options* on page 136 for more information.
- To reload all running instances of *VNC Server* for the current user, in any mode, run the command `vnclicense -reload`. To reload all running instances of *VNC Server* in any mode for all users, run the same command with elevated privileges.

Specifying Xvnc options

The information in this section applies to *VNC Server* in Virtual Mode under UNIX only.

In Virtual Mode, *VNC Server* is both:

- An X server, with a virtual display. To configure it, specify Xvnc options; run the command `vncserver-virtual -list` to see a list of valid options, and examine the output at the top. Note that many of these options may also be valid for your actual X server; run the command `man Xserver` for a more detailed explanation of shared options.
- A standard VNC server. To configure it, specify VNC parameters in the same way as for any other VNC application; start with *Specifying VNC parameters* on page 130.

To compare *VNC Server* modes, consult *Running VNC Server on page 78*.

Configuring VNC Server prior to start up

You can specify Xvnc options in one or more Xvnc configuration files.

When VNC is installed, `/etc/vnc/config` is created; this file is reserved for use by RealVNC. To specify Xvnc options for all user accounts on the computer, create the following file:

```
/etc/vnc/config.custom
```

If this file exists, `/etc/vnc/config` is ignored.

To specify Xvnc options for a particular user account, create the following file:

```
~/.vnc/config
```


If this file exists, it is applied in addition to either `/etc/vnc/config` or `/etc/vnc/config.custom`. Note if you specify the same Xvnc option in multiple locations there is no guarantee which will actually take effect.

Note: `~/ .vnc/config` is ignored if *VNC Server* is started with the `-config FILE` switch; see *Configuring VNC Server at start up* on page 137.

Format of an Xvnc configuration file

Each option in an Xvnc configuration file should be on a separate line, and in the format expected by the X Window System; white space and comments are stripped, and environment variables expanded. For example:

```
#This is a comment
-dumbSched
+kb
-core
+xinerama
nologo
```

Note: RealVNC recommends you do not put VNC parameters in Xvnc configuration files.

Configuring VNC Server at start up

You can pass Xvnc options in at the command line when you start *VNC Server*. RealVNC recommends using the `vncserver-virtual` command or the `vncserver` symlink to start the Xvnc process; options are passed directly to Xvnc without alteration. For example:

```
vncserver-virtual -xinerama -logo
```

Xvnc options specified at the command line are applied in addition to those in any Xvnc configuration files; see *Configuring VNC Server prior to start up* on page 136. Note if you specify the same Xvnc option in multiple locations there is no guarantee which will actually take effect.

Note: If the `-config FILE` command line switch is applied, `~/ .vnc/config` is ignored. Visit www.realvnc.com/products/vnc/documentation/latest/reference/vncserver-virtual.html for more information.

Preventing users configuring VNC

By default, users can configure VNC applications.

If you have:

- An Enterprise license, you can set policy to lock down any VNC application to prevent change. See *Setting policy to lock down VNC applications* on page 138.
- A Personal or a Free license, you can set policy to lock down *VNC Viewer*. You cannot lock down *VNC Server*, though you can make it harder to change. See *Mitigating against change* on page 139.
- Multiple computers with a mix of license types, you can lock down *VNC Server* on computers that have an Enterprise license, and then prevent *VNC Server* running on computers that have a Personal and a Free license. For more information, visit www.realvnc.com/products/vnc/deployment/policy/.

Setting policy to lock down VNC applications

You can specify VNC parameters in special policy Registry keys (Windows) or VNC configuration files (other platforms) in order to lock down VNC applications. Parameters in these locations are applied after all others, overriding the same parameters specified elsewhere, and cannot be changed by users.

Note: Policy template files containing VNC parameters for each application are freely available to download from the RealVNC web site. Visit www.realvnc.com/download/deployment/policy/ for more information.

Windows

VNC application	Registry key mandating policy...
VNC Server in Service Mode	HKLM\Software\Policies\RealVNC\vnserver
VNC Server in User Mode	HKCU\Software\Policies\RealVNC\vnserver
VNC Viewer	HKCU\Software\Policies\RealVNC\vnviewer

It is possible to create policy Registry keys manually; see *Populating the Windows Registry with VNC parameters* on page 131. However, RealVNC recommends downloading policy template files, making the necessary edits, and then using Microsoft tools such as Group Policy to distribute GPOs to target computers.

Note: Set appropriate permissions on `HKLM\Software\Policies\RealVNC` and `HKCU\Software\Policies\RealVNC` to ensure users cannot edit policy Registry keys.

UNIX

VNC application	VNC configuration file mandating policy...	Notes
VNC Server in User Mode	/etc/vnc/policy.d/vncserver-x11	Note both modes share the same file so it is not possible to lock them down separately.
VNC Server in Service Mode		
VNC Server in Virtual Mode	/etc/vnc/policy.d/Xvnc	
VNC Server in Virtual Mode daemon	/etc/vnc/policy.d/vncserver-virtuald	Note parameters related to individual sessions should be specified in /etc/vnc/policy.d/Xvnc, above; see <i>this table</i> on page 132 for why.
VNC Viewer	/etc/vnc/policy.d/vncviewer	

It is possible to create policy VNC configuration files manually; see *Populating VNC configuration files with VNC parameters* on page 132. However, RealVNC recommends downloading policy template files, making the necessary edits, and then distributing files to the /etc/vnc/policy.d directory of target computers.

Note: Set appropriate ownership or permissions on the /etc/vnc/policy.d directory to ensure users cannot edit policy VNC configuration files.

Mac OS X

VNC application	VNC configuration file mandating policy...	Notes
All VNC applications	/etc/vnc/policy.d/common	
VNC Server in Service Mode	/etc/vnc/policy.d/vncserver	Note both modes share the same file so it is not possible to lock them down separately.
VNC Server in User Mode		
VNC Viewer	/etc/vnc/policy.d/vncviewer	

It is possible to create policy VNC configuration files manually; see *Populating VNC configuration files with VNC parameters* on page 132. However, RealVNC recommends downloading policy template files, making the necessary edits, and then distributing files to the /etc/vnc/policy.d directory of target computers.

Note: Set appropriate ownership or permissions on the /etc/vnc/policy.d directory to ensure users cannot edit policy VNC configuration files.

Mitigating against change

Most VNC applications have an **Options** dialog that users can use to make changes; see *Using the Options dialog* on page 135 for more information.

Disabling the VNC Server Options dialog

You can disable the VNC Server **Options** dialog. To do this, specify the `DisableOptions` VNC parameter:

- Under Windows, in the `HKEY_LOCAL_MACHINE\Software\RealVNC\vncserver` (Service Mode) or `HKEY_CURRENT_USER\Software\RealVNC\vncserver` (User Mode) Registry key.
- Under UNIX, in the `/root/.vnc/config.d/vncserver-x11` (Service Mode), `~/.vnc/config.d/vncserver-x11` (User Mode), or `~/.vnc/config.d/Xvnc` (Virtual Mode) VNC configuration file.

- Under Mac OS X, in the `/var/root/.vnc/config.d/vncserver` (Service Mode) or `~/.vnc/config.d/vncserver` (User Mode) VNC configuration file.

Note: Under UNIX and Mac OS X, you can disable the **Options** dialog for all modes and users by specifying the `DisableOptions` parameter in a global location such as `/etc/vnc/config.d/common.custom`.

Disabling the VNC Viewer Options dialog

You cannot disable the *VNC Viewer* **Options** dialog. However, you can set policy to lock down *VNC Viewer* irrespective of license.

Preventing users editing storage locations

VNC parameters and other settings are stored in the locations listed below. Files and directories should have suitable ownership or permissions to prevent users making changes.

Note: Connected users have administrative permissions on a computer if such a user account is currently logged on (Service Mode, User Mode) or was used to start *VNC Server* (Virtual Mode).

Windows

Registry key	Notes
HKEY_LOCAL_MACHINE\Software\RealVNC	
HKEY_CURRENT_USER\Software\RealVNC	For each user account running VNC applications.

UNIX

Directory or file	Notes
<code>/etc/vnc/config.d/</code>	
<code>/etc/vnc/config</code>	<i>VNC Server</i> in Virtual Mode only.
<code>/etc/vnc/config.custom</code>	<i>VNC Server</i> in Virtual Mode only.
<code>/root/.vnc/config.d/</code>	
<code>~/.vnc/config.d/</code>	For each user account running VNC applications.
<code>~/.vnc/config</code>	For each user account running <i>VNC Server</i> in Virtual Mode only.

Mac OS X

Directory	Notes
<code>/etc/vnc/config.d/</code>	
<code>/var/root/.vnc/config.d/</code>	
<code>~/.vnc/config.d/</code>	For each user account running VNC applications.

Managing system authentication

If you have an Enterprise or a Personal license, *VNC Server* is set to use system authentication out-of-the-box. For more information, see *Authenticating using system credentials* on page 96.

Under Windows and Mac OS X, providing the host computer is successfully joined to a domain, there should be no need to configure system authentication. Under UNIX, however, connecting users are by default only able to supply the credentials of *local* user accounts in order to authenticate to *VNC Server*. To enable connecting users to supply the credentials of domain accounts, you must configure both *VNC Server* and the host computer.

Setting up domain accounts under UNIX

When *VNC Server* is installed, a suitable PAM library checking credentials against the local database store is automatically referenced. To see which library this is, and also the default authorization and account rules specified, examine the following file:

- Under modern versions of Linux: `/etc/pam.d/vncserver`.
- Under Solaris, HP-UX, and older versions of Linux: `/etc/pam.conf` (see lines starting `vncserver`).

Note: Under AIX, *VNC Server* uses LAM by default; contact Technical Support for more information. To use PAM, specify the `UsePam` parameter; visit www.realvnc.com/products/vnc/documentation/latest/parameters/vncserver.html#usepam for more information.

To check credentials against an LDAP or an Active Directory password store:

1. Obtain a PAM library that provides this functionality, for example `libpam-krb5.so`. Running the command `vncinitconfig -pam` may help find a suitable library already in use on your system.
2. Reference that library, and specify appropriate account and authentication rules, in the following file:
 - For platforms using `/etc/pam.d/vncserver`, in `/etc/pam.d/vncserver.custom`. Create this file if it does not exist.
 - For platforms using `/etc/pam.conf`: edit this same file to create `vncserver.custom` rules pointing to the new PAM library.
3. In an appropriate system-wide VNC configuration file (for example `/etc/vnc/config.d/common.custom`), specify the following VNC parameter to register your changes with *VNC Server*:

```
PamApplicationName=vncserver.custom
```

For more information on VNC configuration files, see *Configuring VNC applications before they start* on page 131. For more information on this parameter, visit www.realvnc.com/products/vnc/documentation/latest/parameters/vncserver.html#pamapplicationname.

Note that a suitable PAM library for your platform may already be installed on the host computer, and appropriate account and authentication rules specified. For example, if your system has been Kerberized, or third party software such as Centrify or PowerBroker Identity Services installed to integrate with Active Directory, then you may be able to simply reference changes already made. For example, under Debian-compatible Linux, you may be able to edit `/etc/pam.d/vncserver.custom` as follows:

```
@include common-auth
@include common-account
@include common-session
```

For Red Hat-compatible Linux, the equivalent edits might be:

```
auth      include    password-auth
account   include    password-auth
session   include    password-auth
```

Registering domain accounts with VNC Server

Domain accounts must be registered with *VNC Server* in the standard way, using either:

- The `Permissions` parameter; visit www.realvnc.com/products/vnc/documentation/latest/parameters/vncserver.html#permissions.
- The user interface; see *Managing the list of registered user accounts and groups* on page 97.

You may need to qualify user names with the domain name, for example `DEV.ACMECORP.COM\johndoe`. Note that connecting users may also need to supply the user name qualified in this way too.

Setting up single sign-on authentication

If you have an Enterprise license, you can specify single sign-on as the authentication scheme for *VNC Server*. See *Authenticating users automatically* on page 100 for more information.

Note the following conditions, which may mean that single sign-on is unsuitable for use in a home or small office environment:

- All prospective client and host computers must be joined to the same domain (a network managed by a domain controller, running specialized software such as Kerberos or Active Directory).
- All prospective *VNC Viewer* users must log on to their client computers using the credentials of domain accounts; that is, of user accounts managed by the domain controller.
- A fallback authentication scheme must be provided in case single sign-on fails for any reason. See *Providing a fallback scheme* on page 143.

Setting up the host computer

Perform the following steps:

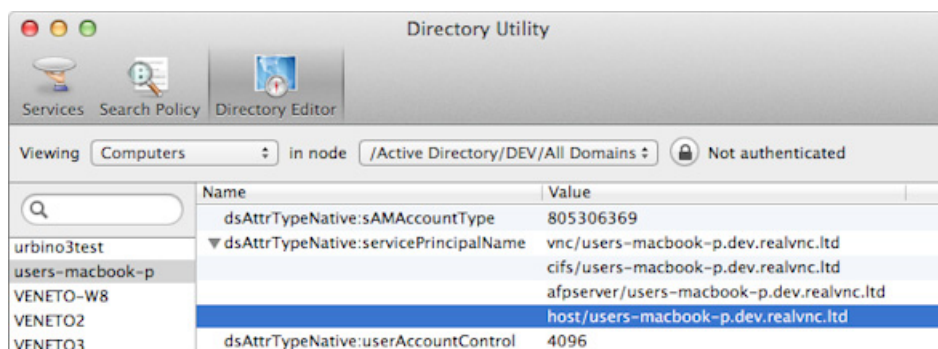
1. Make sure the host computer is joined to a domain.
2. Specify the single sign-on authentication scheme, using either:
 - The `Authentication VNC` parameter; visit www.realvnc.com/products/vnc/documentation/latest/parameters/vncserver.html#authentication.
 - The user interface; see *Authenticating users automatically* on page 100.
3. Under UNIX and Mac OS X, obtain a GSSAPI-compatible library.

Note a suitable library may already be present on your system, for example `/usr/lib/x86_64-linux-gnu/libgssapi_krb5.so` under Ubuntu Linux, or `/usr/lib/libgssapi_krb5.dylib` under Mac OS X. Alternatively, you may be able to obtain one by installing third party software such as PowerBroker Identity Services or Centrify, designed to integrate with Active Directory.

4. Under UNIX and Mac OS X, create an `/etc/vnc/ssolib` symbolic link pointing to the location of the GSSAPI-compatible library (above).
5. Under Mac OS X 10.7 only, if you are integrating with Active Directory, edit the `/etc/pam.d/authorization` file as follows:

```
auth    optional    pam_krb5.so use_first_pass use_kcminit default_principal
auth    sufficient   pam_krb5.so use_first_pass default_principal
auth    optional    pam_ntlm.so use_first_pass
auth    required     pam_opendirectory.so use_first_pass nullok
account required    pam_opendirectory.so
```

6. Under Mac OS X 10.7 onwards, use Directory Utility (`/System/Library/CoreServices/Directory Utility.app`) to ascertain the service principal name of the host computer as it is registered with the domain controller, for example:



Assign the `dsAttrTypeNative:servicePrincipalName` 'host' value to the VNC Server `KerberosPrincipalName` parameter, so in this case `host/users-macbook-p.dev.realvnc.ltd`.

7. Register the domain accounts of all prospective VNC Viewer users with VNC Server, using either:
 - The Permissions VNC parameter; visit www.realvnc.com/products/vnc/documentation/latest/parameters/vncserver.html#permissions.
 - The user interface; see *Managing the list of registered user accounts and groups* on page 97.

Note you may need to qualify user names with the domain name, for example `DEV.ACMECORP.COM\johndoe`.

Providing a fallback scheme

If single sign-on fails for any reason (for example, the domain controller cannot be contacted), VNC Server automatically falls back to the authentication scheme specified by the `Authentication VNC` parameter. By default, this is system authentication, and connecting users are prompted to supply the credentials of a user account valid for logging on to the host computer.

By default under UNIX, connecting users are only able to supply the credentials of local user accounts. To enable connecting users to supply their own credentials (that is, of domain accounts), you must configure both *VNC Server* and the host computer. Follow the instructions in *Managing system authentication* on page 141.

Setting up each client computer

Perform the following steps:

1. Make sure the client computer is joined to the same domain as the host computer.
2. Make sure the *VNC Viewer* user logs on to their client computer using the credentials of a domain account.
3. Under UNIX and Mac OS X, obtain a GSSAPI-compatible library.

Note a suitable library may already be present on your system, for example `/usr/lib/x86_64-linux-gnu/libgssapi_krb5.so` under Ubuntu Linux, or `/usr/lib/libgssapi_krb5.dylib` under Mac OS X. Alternatively, you may be able to obtain one by installing third party software such as PowerBroker Identity Services or Centrify, designed to integrate with Active Directory.
4. Under UNIX and Mac OS X, create an `/etc/vnc/ssolib` symbolic link pointing to the location of the GSSAPI-compatible library (above).
5. Make sure *VNC Viewer* is set to use single sign-on, by either:
 - Setting the `SingleSignOn` VNC parameter to `TRUE`; visit www.realvnc.com/products/vnc/documentation/latest/parameters/vncviewer.html#singlesignon.
 - Turning on **Use single sign-on if VNC Server supports it** in the *VNC Viewer Options* dialog); see page 38.

Hosting VNC on a UNIX network share

This section explains how to install VNC applications on one UNIX computer and run those applications from any other UNIX computer with whom the installation directory is shared.

Note the following restrictions, which may mean that certain VNC applications or *VNC Server* modes cannot be hosted in this way:

- A domain license key is required for *VNC Server*. Contact RealVNC for more information.
- *VNC Server* in Service Mode (`vncserver-x11-serviced`) and the *VNC Server* in Virtual Mode daemon (`vncserver-virtuald`) are not supported.
- If system authentication is specified, connecting users can only authenticate using the credentials of the host computer user starting *VNC Server*. The credentials of other local user accounts registered using the `Permissions` VNC parameter are ignored.
- The single sign-on authentication scheme is not available.
- Printing is not available.
- The `vncserver` symlink is not available to start *VNC Server* in Virtual Mode out-of-the-box.

To host VNC applications (note all commands require administrative privileges):

1. *On the hosting computer*, download generic installer(s) containing unpackaged binaries from www.realvnc.com/download/vnc/, and extract to *<install dir>*. Navigate to this directory, but do not run the `vncinstall` script.

Note: Choose a generic installer appropriate to the platform and architecture of the computers you intend to share the installation directory with (that is, from which VNC applications will be run). For example, if you are targeting a mixture of Ubuntu computers, you could download both **VNC for Linux** generic installers, and create and share *<install dir>/x86* and *<install dir>/x64* appropriately.

2. Create an *<install dir>/vnc* directory.
3. Run the following command to license VNC Server:

```
vnclicense -LicenseDir=<install dir>/vnc -add <domain license key>
```

4. Run the command `vncinitconfig -config` to generate a font path for virtual desktops, and move the resulting `/etc/vnc/config` file to *<install dir>/vnc*.

Note: This path is extracted from the X server of the hosting computer. If computers from which applications will be run have a different X server configuration, it may be necessary to create an `/etc/vnc/config.custom` file on each, and populate it with the `Font Path` output of the command `xset -q`.

5. Run the command `vncinitconfig -xstartup` to generate a start up script for virtual desktops, and move the resulting `/etc/vnc/xstartup` file to *<install dir>/vnc*.
6. *On each computer from which applications will be run*, mount *<install dir>* read-only, and add the location to users' paths.

Configuring VNC applications centrally

You can configure VNC applications using VNC parameters, and additionally VNC Server in Virtual Mode using Xvnc options. See *Configuring VNC* on page 130 for general information.

Specifying VNC parameters

You can specify VNC parameters in one or more VNC configuration files. VNC configuration files have a strict hierarchy; see *Populating VNC configuration files with VNC parameters* on page 132 for more information, a full list of files, and the order in which parameters are applied.

VNC configuration files must be located in directories under *<install dir>/vnc*. Perform the following steps:

1. Create an *<install dir>/vnc/config.d* directory, and move `/etc/vnc/config.d/common` to it. This file is reserved for use by RealVNC.
2. Create an *<install dir>/vnc/policy.d* directory if you want to set policy. See *Setting policy to lock down VNC applications* on page 138 for more information.
3. Create and populate with VNC parameters as many of the following files as required:

To configure...	Create and populate...
All VNC applications that can be served	<i><install dir>/vnc/config.d/common.custom</i>
	<i><install dir>/vnc/policy.d/common</i>

To configure...	Create and populate...
VNC Server in User Mode (vncserver-x11)	<install dir>/vnc/config.d/vncserver-x11
	<install dir>/vnc/policy.d/vncserver-x11
VNC Server in Virtual Mode (Xvnc, via vncserver-virtual)	<install dir>/vnc/config.d/Xvnc
	<install dir>/vnc/policy.d/Xvnc
VNC Viewer (vncviewer)	<install dir>/vnc/config.d/vncviewer
	<install dir>/vnc/policy.d/vncviewer

Note the following:

- If you specify a default configuration in <install dir>/vnc/config.d, individual users on computers running VNC applications can override your preferences by specifying the same VNC parameters at the command line when applications start. To prevent this, set policy.
- If you specify a default configuration in <install dir>/vnc/config.d, individual users on computers running VNC applications can persist changes they make via **Options** dialogs, since these changes are written to VNC configuration files in ~/.vnc/config.d, and reloaded each time the applications run. To prevent this, set policy.
- If computers running VNC applications have VNC configuration files stored locally in /etc/vnc/config.d (perhaps because VNC was previously installed), VNC parameters in those files override the same parameters specified in <install dir>/vnc/config.d. To prevent this, remove this directory from affected computers, or set policy.
- If computers running VNC applications have policy set locally in /etc/vnc/policy.d (perhaps because VNC was previously installed), VNC parameters in those files override the same parameters specified in <install dir>/vnc/policy.d. To prevent this, remove this directory from affected computers.

Specifying Xvnc options

You can specify Xvnc options for VNC Server in Virtual Mode in an Xvnc configuration file. See *Specifying Xvnc options* on page 136 for why you might want to do this.

Note: RealVNC recommends you do not put VNC parameters in Xvnc configuration files.

To do this, create <install dir>/vnc/config.custom and populate it with valid Xvnc options. Note options in this file override the same options specified by RealVNC in <install dir>/vnc/config.

Note the following:

- If you specify Xvnc options in <install dir>/vnc/config.custom, individual users on computers running VNC Server in Virtual Mode can override your preferences by appending Xvnc options to the vncserver-virtual command.
- If computers running VNC Server in Virtual Mode have either the /etc/vnc/config or /etc/vnc/config.custom Xvnc configuration files stored locally (perhaps because VNC was previously installed), Xvnc options in these files override the same options specified in <install dir>/vnc/config.custom. To prevent this, remove these files from affected computers.

- If individual users have a `~/ .vnc/config` Xvnc configuration file stored locally (perhaps because VNC was previously installed), Xvnc options in this file override the same options specified in `<install dir>/vnc/config.custom`. To prevent this, remove this file from affected computers.

Logging information

By default, *VNC Server* and *VNC Viewer* record basic information about connection activity. You can increase the amount of information recorded, change the type of activity, or alter the destination. In addition, you can start recording information about other VNC applications and processes.

The following table lists the default destinations for *VNC Server* and *VNC Viewer* log output:

Application		Windows	Mac OS X	UNIX
VNC Server	Service Mode	Event Log (see note 3)	syslog	syslog, to the USER facility (see note 5)
	User Mode	C:\Users\<user>\AppData\Local\RealVNC\vncserver.log (see note 4)	~/Library/Logs/vnc/vncserver.log	~/ .vnc/vncserver-x11.log
	Virtual Mode	—	—	Standard Error (see note 6)
	Virtual Mode daemon	—	—	syslog, to the DAEMON facility (see also note 7)
VNC Viewer		Standard Error	Standard Error	Standard Error

Note the following:

1. If the destination is to file, the location is determined by the `LogDir` and `LogFile` VNC parameters. Containing directories must be writable. Start with www.realvnc.com/products/vnc/documentation/latest/parameters/vncserver.html#log.
2. If the destination is to file, file contents are overwritten each time an application is restarted. To preserve information, choose a different destination, for example Standard Error. (You could still redirect this to file, for example by using a command such as `vncserver-x11 -Log=:stderr:100 2>>myfile`.)
3. Under Windows, you must ensure the Windows Event Log service is running and that **Event Viewer > Windows Logs > Application > Properties** is set to overwrite as needed. If the service is not running or the event log is full, connections cannot be established.
4. This location is for Windows 7, though note `AppData` may be hidden by default. The location is slightly different under some other versions of Windows.
5. Under UNIX, *VNC Server* in Service Mode can be configured to log to different facilities using the `SyslogFacility` parameter.
6. Under UNIX, the default destination for *VNC Server* in Virtual Mode is Standard Error, but `vncserver-virtual` (or the `vncserver` symlink) automatically redirects this to file at `~/ .vnc/<computer>:<display number>.log`. Note the output of the X server session is included.

- Under UNIX, each time a user connects to the *VNC Server* in Virtual Mode daemon, a new instance of *VNC Server* in Virtual Mode is immediately started, and its log output automatically redirected to file as above.

Note: Under UNIX and Mac OS X, *VNC Server* also automatically logs connections authenticated using the system authentication or single sign-on schemes to the syslog AUTHPRIV facility, typically located at `/var/log/auth.log` and `/var/log/secure.log` respectively.

Changing the information recorded

To change the content, destination, and quality of information recorded, edit the `Log VNC` parameter.

See *Specifying VNC parameters* on page 130 for an introduction to VNC parameters. Start with www.realvnc.com/products/vnc/documentation/latest/parameters/vncserver.html#log for valid values for the *VNC Server* `Log` parameter.

Quickly generating debug logs

You may be eligible to contact Technical Support if you encounter a problem or require assistance. See *Contacting Technical Support* on page 8 for more information.

The Technical Support team rely on comprehensive debug log files to troubleshoot problems, equivalent to setting the *VNC Server* and *VNC Viewer* `Log` parameters to `*:file:100`.

In order to quickly generate a debug log file for either *VNC Server* or *VNC Viewer*:

- On the **Troubleshooting** page of the **Options** dialog, choose **Create a debug log file**, and then **OK**.
- Restart the application.
- Recreate the problem, and send the file in the specified location to Technical Support.

Recording information about other applications and processes

You can apply the `Log`, `LogFile`, and `LogDir` VNC parameters to VNC applications other than *VNC Server* and *VNC Viewer*, and also to *VNC Server* sub-processes. This may be useful if Technical Support requests that you dig deeper into any problems you may encounter.

Windows

You can apply parameters to the following applications and sub-processes by creating special keys in the Windows Registry. Alternatively, for some applications, you can apply parameters at the command line.

Application or sub-process			Registry key	Parameters can be applied...	Registry hive
VNC Server	Service Mode	User interface	vncserverui-service	Registry	HKEY_CURRENT_USER
	User Mode	User interface	vncserverui-user		
Licensing	(command line)		vnclicense	Registry or command line	
	(Wizard)		vnclicensewiz		
VNC Address Book			vncaddrbook		

For example, to create a log file for the *VNC Server* in Service Mode user interface:

1. Using Registry Editor, navigate to `HKEY_CURRENT_USER\Software\RealVNC`.
2. Select **New > Key** from the shortcut menu, and create `vncserverui-service`.
3. Select **New > String Value** from the shortcut menu, and create `Log`.
4. Select **Modify** from the shortcut menu, and specify appropriate **Value data**, for example `*:file:100`.

Repeat steps 3 and 4 for the `LogFile` and `LogDir` parameters, if necessary. Restart the application to create the new log file.

To create a log file for an application at the command line, apply parameters before any command, for example:

```
vnclicense.exe -Log=*:file:100 -LogFile=license.log -add <key>
```

UNIX

You can apply parameters to the following applications when run from the command line:

```
vnclicense, vnclicensewiz, vncaddrbook
```

Do so before any command, for example:

```
vnclicense -Log=*:file:100 -LogDir=/home/dev/logs -add <key>
```

Mac OS X

You can apply the logging parameters to the following applications when run from the command line:

```
vnclicense, vnclicensewiz
```

Do so before any command, for example:

```
/Library/vnc/VNC\ Server\ Licensing.app/Contents/MacOS/vnclicensewiz  
-Log=*:file:100
```

Note: Two files are created for the *VNC Server Licensing Wizard*: `~/Library/Logs/vnc/vnclicensewiz.log` and `/Library/Logs/vnclicensewiz_helper.log`.

Completely removing VNC

To completely remove *VNC*, first run the *VNC* uninstaller(s) in the standard way for your operating system. Follow the appropriate instructions at www.realvnc.com/products/vnc/documentation/latest/installing-removing/.

The *VNC* uninstaller(s) remove all program files, and security-related files and settings. This section lists the (benign) files and settings that remain. It assumes an original installation to the default location.

Appendix B: Setting Up VNC

Windows

Registry key or other setting	Notes
HKEY_LOCAL_MACHINE\Software\RealVNC	
HKEY_LOCAL_MACHINE\Software\Policies\RealVNC	
HKEY_CURRENT_USER\Software\RealVNC	For each user account running VNC applications
HKEY_CURRENT_USER\Software\Policies\RealVNC	For each user account running VNC applications
C:\Users\~\.vnc\	For each user account running VNC applications
A firewall entry for <i>Listening VNC Viewer</i>	If one was created

Note: *VNC Mirror Driver* has been uninstalled if it is no longer listed as a display adaptor in Windows Device Manager. Note any remaining files are managed by Windows as part of the Driver Store and should not be manually removed.

UNIX

Directory or file	Notes
/etc/vnc/	
/root/.vnc/	
~/.vnc/	For each user account running VNC applications
/etc/pam.d/vncserver*	
/etc/init.d/vncserver*	Linux distributions using <code>initd</code>
/etc/rc*.d/*vncserver*	Linux distributions using <code>initd</code>
/usr/lib/systemd/system/vncserver*	Linux distributions using <code>systemd</code>
/var/log/vncserver*	
/tmp/.vnc*	

Note: *VNC Server* in Virtual Mode creates a `/tmp/.X11-unix` directory and `/tmp/.X<num>` files that may persist after the application stops. Run the command `vncserver-virtual -clean` before uninstalling VNC to delete stale files.

Mac OS X

Directory or file	Notes
/etc/vnc/	
/var/root/.vnc/	
~/.vnc/	For each user account running VNC applications
/etc/pam.d/vncserver*	
/Library/Logs/vnc*.log	
~/Library/Logs/vnc	For each user account running VNC applications
/Library/LaunchAgents/*realvnc*.plist	

Directory or file	Notes
/Library/LaunchDaemons/*realvnc*.plist	
~/Library/Preferences/*realvnc*.plist	For each user account running VNC applications
/tmp/.vnc*	

