Trademarks

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

Protected by UK patent 2481870.

Copyright

Copyright © RealVNC Limited, 2002-2012. 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 the 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 33
- Starting VNC Viewer 34
- Starting Listening VNC Viewer 34
- Configuring VNC Viewer before you connect 35
- Connecting to a host computer 37
- The VNC Viewer user experience 38
- Using the toolbar 40
- Using the shortcut menu 41
- Using the VNC Viewer - Options dialog 42
- Managing the current connection 43
- Changing appearance and behavior 44
- Restricting access to features 46
<table>
<thead>
<tr>
<th>Chapter 4: Connecting From A Web Browser</th>
<th>49</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connecting to a host computer</td>
<td>50</td>
</tr>
<tr>
<td>The VNC Viewer for Java user experience</td>
<td>54</td>
</tr>
<tr>
<td>Working with VNC Viewer for Java</td>
<td>55</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 5: Exchanging Information</th>
<th>59</th>
</tr>
</thead>
<tbody>
<tr>
<td>Printing host computer files to a local printer</td>
<td>60</td>
</tr>
<tr>
<td>Transferring files between client and host computers</td>
<td>62</td>
</tr>
<tr>
<td>Copying and pasting text between client and host computers</td>
<td>66</td>
</tr>
<tr>
<td>Communicating securely using chat</td>
<td>67</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 6: Setting Up VNC Server</th>
<th>71</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licensing VNC Server</td>
<td>72</td>
</tr>
<tr>
<td>Starting VNC Server</td>
<td>73</td>
</tr>
<tr>
<td>Running multiple instances of VNC Server</td>
<td>78</td>
</tr>
<tr>
<td>Working with VNC Server</td>
<td>81</td>
</tr>
<tr>
<td>Configuring ports</td>
<td>88</td>
</tr>
<tr>
<td>Notifying when users connect</td>
<td>91</td>
</tr>
<tr>
<td>Preventing connections to VNC Server</td>
<td>92</td>
</tr>
<tr>
<td>Restricting functionality for connected users</td>
<td>93</td>
</tr>
<tr>
<td>Stopping VNC Server</td>
<td>95</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 7: Making Connections Secure</th>
<th>97</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticating connections to VNC Server</td>
<td>98</td>
</tr>
<tr>
<td>Relaxing the authentication rules</td>
<td>104</td>
</tr>
<tr>
<td>Bypassing the authentication rules</td>
<td>107</td>
</tr>
<tr>
<td>Changing the encryption rules</td>
<td>109</td>
</tr>
<tr>
<td>Preventing particular connections to VNC Server</td>
<td>111</td>
</tr>
<tr>
<td>Restricting features for particular connected users</td>
<td>114</td>
</tr>
<tr>
<td>Uniquely identifying VNC Server</td>
<td>118</td>
</tr>
<tr>
<td>Protecting privacy</td>
<td>118</td>
</tr>
</tbody>
</table>
Appendix A: Saving Connections 121

- Saving connections to VNC Address Book 122
- Using VNC Address Book to connect 127
- Managing connections using VNC Address Book 128
- Saving connections to desktop icons 131
About This Guide

This Guide explains how to use VNC 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 licensed to use VNC Server (Enterprise). Unless otherwise stated, this combination is assumed. To see how to set these applications up, read Getting the computers ready to use on page 11.

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

VNC Server (with different licenses applied)

- VNC Server (Personal)
  Contains most RealVNC remote control features. A thirty day trial is available.

- VNC Server (Free)
  Contains basic remote control features.

For more information on licensing VNC Server, start with Licensing VNC Server on page 72.

VNC Viewer

- VNC Viewer for Java
  This application is freely available to download on demand from VNC Server (Enterprise) or VNC Server (Personal).

- VNC Viewer Plus
  This application is available to purchase from www.realvnc.com/products/viewerplus/.

- VNC Viewer for iOS
  This application is available to purchase from the Apple App Store. Visit www.realvnc.com/products/ios/ for more information.

- VNC Viewer for Android
  This application is available to purchase from Google Play. Visit www.realvnc.com/products/android/ 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.
About This Guide

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.

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

Technical Support

You can contact Technical Support if you have a valid support and upgrades contract to use VNC Server (Enterprise) or VNC Server (Personal). To see whether this is the case, examine the Details section of the VNC Server dialog, or run the command vnclicense -list.

For more information, visit www.realvnc.com/support/.

Related information

Visit www.realvnc.com for:

• Supported platforms, operating systems, and system requirements.
• Instructions on how to install and uninstall VNC.
• Release notes, Knowledge Base articles, forums, and FAQs.
• Information relating to earlier incarnations of VNC.
• Information relating to other RealVNC products and solutions.
Introduction

This Guide summarizes how to use VNC 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 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 licensed to use VNC Server (Enterprise). For a list of other products and license types to which some information may also apply, see Applicable software on page 7.

Contents

Principles of VNC remote control 10
Getting the 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 obtain the latest version of **VNC Server**, download VNC from www.realvnc.com/download/vnc/. Follow the instructions to license it, or consult **Licensing VNC Server** on page 72.

  **Note:** You may be able to control computers running alternatives to **VNC Server**. For more information, see **Connecting to VNC-compatible Server applications** 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. The latest version of **VNC Viewer** is available to download from www.realvnc.com/download/viewer/.

  **Note:** You may be able to control computers 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.

For information on how to set these applications up, see **Getting the computers ready to use** on page 11.

Consider the following example environment:

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. 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 permits other users to connect to the host computer at the same time as you. You may be sharing control.

VNC 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 the 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 (3G/GPRS/EDGE).
2. Download and install VNC from www.realvnc.com/download/vnc/, and license the VNC Server component. The credentials of a user with administrative privileges on the host computer are required. For more information on licensing, start with Licensing VNC Server on page 72.
3. If you are connecting over a public network such as the Internet, it is very likely the host computer will be protected by at least one firewall. If so, each must be configured to allow network communications through to the port on which VNC Server is listening, which is 5900 by default. See Allowing network communications through a firewall on page 31 for more information.
4. If you are connecting over a public network such as the Internet, it is very likely the host computer will be protected by at least one router. If so, each must be configured to forward network communications through to the port on which VNC Server is listening, which is 5900 by default. See Configuring a router to forward network communications on page 29.
Chapter 1: Introduction

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 must be a private address, which is that of the host computer itself. See Connecting within a private network on page 27 for more information.
   — Over the Internet, this must be a public address, which is that of a router or similar device. See Connecting over the Internet on page 28 for more information.

7. Find out the credentials required to authenticate to VNC Server. By default, if you are connecting to:
   — VNC Server (Enterprise) or VNC Server (Personal), you require the user name and password of a user account with administrative privileges on the host computer. Note at least one account on the host computer must have a password set; see Authenticating using host computer user credentials on page 98 for more information.
   — VNC Server (Free), you require a password specific to VNC. For more information, see Authenticating using a VNC password on page 103.

   Note: If you cannot perform these operations and a host computer user is present, you may be able to jointly perform a reverse connection. See Establishing a reverse connection on page 107 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.

2. Download VNC Viewer 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>

   Note: Alternatively, you can download and install VNC on the client computer, and just run the VNC Viewer component, since it does 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.

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 36.
Connectivity and feature matrix

You can use VNC Viewer to connect to:

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

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

Note: This section assumes you are connecting from the latest version of VNC Viewer. For alternatives, see Connecting from alternatives to VNC Viewer on page 15.

Connecting to VNC

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

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

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

Restrictions

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

Once a connection is established, you cannot:

- Exchange files with VNC Server (Free).
- Print VNC Server (Free) files.
- Chat with other VNC Server (Free) users.
Chapter 1: Introduction

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 you enter to log on to 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.

<table>
<thead>
<tr>
<th>VNC Viewer</th>
<th>VNC Enterprise Edition 4.5-</th>
<th>VNC Personal Edition 4.5-</th>
</tr>
</thead>
<tbody>
<tr>
<td>On the client computer, VNC Viewer encryption must not be set to Always Maximum.</td>
<td>On the client computer, VNC Viewer encryption must not be set to Always Maximum.</td>
<td></td>
</tr>
</tbody>
</table>

Restrictions

• Connections to VNC Enterprise Edition and VNC Personal Edition cannot be encrypted using ultra-secure 256-bit AES.

• The credentials you enter to log on to 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.
Chapter 1: Introduction

Connecting to VNC-compatible Server applications

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

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

Restrictions

Note that no RealVNC remote control features are available for connections to host computers running VNC-compatible Server applications. 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 for iOS. See Connecting from mobile devices on page 16.
- VNC Viewer for Android. See Connecting from mobile devices on page 16.
- VNC-compatible Viewer applications from third parties. See Connecting from VNC-compatible Viewer software on page 16.

Connecting from VNC Viewer for Java

You can use any modern web browser to download VNC Viewer for Java from VNC Server (Enterprise) or VNC Server (Personal) on demand, and then immediately connect.

Note: You cannot download VNC Viewer for Java from VNC Server (Free).

You do not require the credentials of a user with administrative privileges on the host computer in order to use VNC Viewer for Java. For more information, see Chapter 4, Connecting From A Web Browser on page 49.
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 purchase and install:


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-compatible Viewer software

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

In order to allow connections to VNC Server (Enterprise) or VNC Server (Personal), make sure:

- Encryption is turned off. See Changing the encryption rules on page 109.
- System authentication is turned off. See Relaxing the authentication rules on page 104.

Restrictions

Note that no RealVNC remote control features are available for connections from client computers running VNC-compatible Viewer applications. 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 33.
* If you want to control a host computer from a web browser instead of VNC Viewer, read Chapter 4, Connecting From A Web Browser on page 49.
* To see how to exchange information between client and host computers, read Chapter 5, Exchanging Information on page 59.
* To learn how to configure VNC Server on the host computer, and for advanced topics such as running multiple instances of VNC Server, see Chapter 6, Setting Up VNC Server on page 71.
* By default, VNC Server establishes authenticated and, depending upon your license, encrypted connections. 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 97.
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 licensed to use VNC Server (Enterprise). For a list of other products and license types to which some information 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 the 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, select RealVNC > VNC Server from the Start menu, or double-click the VNC Server desktop icon, if available. Note administrative privileges are required to perform this operation.
- Under UNIX/Linux, select Applications > Internet > VNC Server (User Mode) from the menu system, or search for this application using the standard facility.
  
  **Note:** If no menu system or search facility is available, open a Terminal window, run the command vncserver-x11, and press the ENTER key. Note you should not do this as a user with administrative privileges.
- Under Mac OS X, navigate to the Applications > RealVNC folder, and double-click the VNC Server program. Note administrative privileges are required to perform this operation.

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 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

This section assumes VNC Viewer is available on the client computer. For more information, see Setting up the client computer on page 12.

To start VNC Viewer, double-click an appropriate icon, or open a Command or Terminal window and:

- Under Windows, run the command `<VNC Viewer>.exe`
- Under UNIX/Linux, run the command `./<VNC Viewer>`
- Under Mac OS X, run the command `<VNC Viewer>.app/Contents/MacOS/vncviewer`

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, enter the network address of the host computer itself in the VNC Server dropdown. This address can take the following forms:

- A host name for the host computer, for example `johndoe`. (Note the computer may not have a host name.)
- An IP address for the host computer in IPv4 format, for example `192.168.0.133`
- An IP address for the host computer 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 27.

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/Linux, or if more than one instance of VNC Server is running on the host computer. If, when you try to connect, you see an error message similar to the following:

```
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 VNC Server determines whether or not connections are actually encrypted (requesting encryption is not a guarantee).

**Note:** For more information on encryption, and security in general, see Chapter 7, Making Connections Secure on page 97.

By default, connections to:

- **VNC Server (Enterprise)** are encrypted using industry-standard 128-bit AES. You can request that this be enhanced to ultra-secure 256-bit AES.
- **VNC Server (Personal)** are encrypted using industry-standard 128-bit AES.
- **VNC Server (Free)** cannot be encrypted. Upgrade the host computer to VNC Server (Enterprise) or VNC Server (Personal) if security is important to you.
By default, in the VNC Viewer dialog, the Encryption dropdown is set to Let VNC Server choose:

If you are connecting to:

- VNC Server (Enterprise) or VNC Server (Personal), 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 (Enterprise) only.
  - Turned off.
  For more information on these operations, see Changing the encryption rules on page 109.
- VNC Server (Free), 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.
Chapter 2: Getting Connected

Checking the signature

If you are connecting to VNC Server (Enterprise) or VNC Server (Personal), you may see a message similar to the following:

No signature has been stored for this VNC Server, so its identity cannot be identified.

The VNC Server signature is 2d-99-e9-11-aa-73-e6-f9.

Do you wish to accept the signature and continue connecting?

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 correct destination (and not, for example, to a malicious third party) by comparing this signature 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 you do not connect. For more information on this security feature, see Uniquely identifying VNC Server on page 118.

Click the Yes button to continue connecting to VNC Server.

Acknowledging the encryption status

If the connection is unencrypted, you are prompted to acknowledge that sensitive information may not necessarily be secure:
If this is unacceptable and you are connecting to VNC Server (Enterprise) or VNC Server (Personal), you may be able to turn encryption on. Click the Cancel button and see Changing the encryption rules on page 109 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 (Enterprise) or VNC Server (Personal)**, enter the credentials of a user with administrative privileges on the host computer. If you:
  
  — Do not know such credentials but have access to the host computer, you may be able to find them out, or alternatively register your own credentials. If you do not have access, contact a system administrator or a host computer user.
  
  — Know that the primary user account does not have a password set (likely for friends and family only), then you must change the default authentication mechanism, or disable authentication altogether.

  For more information, start with Authenticating using host computer user credentials on page 98.

- **VNC Server (Free)**, 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 VNC password on page 103 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 38.

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

**Note:** Once connected, you can save the connection details 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 121.
Troubleshooting connection

This section provides additional information to help you connect.
If, after reading this, you still cannot connect:
2. If you have a valid support and upgrades contract to use VNC Server (Enterprise) or VNC Server (Personal), contact Technical Support. Start with Technical Support on page 8 for more information.
3. If all else fails, and providing you are in a secure 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 107.

Licensing VNC Server

VNC Server must be licensed. If it is not, users cannot connect.
Note: VNC Viewer does not need to be licensed.
If VNC Server is not licensed, the status bar on the VNC Server dialog turns red:

![VNC Server dialog with unlicensed status](image)
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 72** 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:
Chapter 2: Getting Connected

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:

![VNC Server dialog]

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:

![VNC Viewer]

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:

```plaintext
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 Configuring ports on page 88.

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
192.168.0.133:1
[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
192.168.0.133::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:
  - 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 192.168.0.133 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 user name or password, and you do not have access to the host computer, you will need to consult your system administrator or a host computer user. If you do have access to the host computer, and sufficient privileges to configure VNC Server, you may be able to relax the authentication rules. For more information, see Relaxing the authentication rules on page 104.

Failing to authenticate as ‘you’

If you see the following error message:

Access is denied.

then VNC Server has been configured to require the credentials of a host computer user. Your user name and password, however, have not been added to the authentication list.

If this is the case and you do not have access to the host computer, you will need to consult your system administrator or a host computer user. If you do have access to the host computer, and sufficient privileges to configure VNC Server, you may be able to register your credentials. For more information, see Managing users and groups in the authentication list on page 102.
Chapter 2: Getting Connected

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 111.

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

If this is the case and you do not have access to the host computer, you will need to consult your system administrator or a host computer user. If you do have access to the host computer, and sufficient privileges to configure VNC Server, you may be able to bypass host computer connection prompts. For more information, see Preventing particular users connecting on page 113.
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 34
Starting Listening VNC Viewer 34
Configuring VNC Viewer before you connect 35
Connecting to a host computer 37
The VNC Viewer user experience 38
Using the toolbar 40
Using the shortcut menu 41
Using the VNC Viewer - Options dialog 42
Managing the current connection 43
Changing appearance and behavior 44
Restricting access to features 46
Starting VNC Viewer

To start VNC Viewer on a client computer, follow the instructions in Step 2: Start VNC Viewer on the client computer on page 21.

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 37.

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 35.

To see how to start VNC Viewer so that it listens for a reverse connection, start with Starting Listening VNC Viewer on page 34.

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 107.

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

To start Listening VNC Viewer, open a Command or Terminal window and:

- Under Windows, run the command <VNC Viewer>.exe -listen.
- Under UNIX/Linux, run the command ./<VNC Viewer> -listen.
- Under Mac OS X, run the command <VNC Viewer>.app/Contents/MacOS/vncviewer -listen.

Note: If you installed VNC on the client computer, you can start Listening VNC Viewer from the menu system of most operating systems, which may be more convenient. See Setting up the client computer on page 12 for more information.
Under Windows and Mac OS X, a VNC Viewer icon is displayed in the Notification area or Status bar. Under Windows 7, note this area is hidden by default and accessible from to the right of the Taskbar. Hover the mouse cursor over the icon to confirm that Listening VNC Viewer is running:

Under Windows and Mac OS X, 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 35.

**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 37.

If a reverse connection:
- Is successfully established, Listening VNC Viewer displays the host computer’s desktop in a new window on the client computer in exactly the same way as VNC Viewer. Carry on from The VNC Viewer user experience on page 38.
- Is not successful, start with Establishing a reverse connection on page 107.

### 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 37.

However, you must 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 36.
- VNC Server mandates the single sign-on authentication mechanism but you do not want to authenticate as the user you logged on to the client computer as. See Disabling single sign-on on page 36.
- You want to specify printing options. See Configuring printing on page 37.
To configure VNC Viewer before you connect, click the **Options** button at the bottom of the VNC Viewer dialog. More on this dialog. The VNC Viewer - Options dialog opens:

![VNC Viewer - Options dialog](image)

(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 this browser has already been provisioned with proxy server information. Note this option has a different name under UNIX/Linux and Mac OS X.
- **Use these proxy settings** to specify the network address of either an HTTP or a SOCKS 5 proxy server, and a port on which an appropriate application or process is listening, separated by a colon.
  
  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 VNC Viewer for Windows and Mac OS X, for connections to VNC Server (Enterprise) only.

By default, if VNC Server (Enterprise) specifies single sign-on as its authentication mechanism, then you may be able to connect without supplying a user name and password. This is because you have already
Chapter 3: Using VNC Viewer

successfully authenticated to a network when logging on to your client computer. For more information, see *Authenticating automatically using client computer user credentials* on page 105.

You can disable this feature if you want to connect to VNC Server using the credentials of a different user. This might give you access to more VNC 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 (Enterprise) or VNC Server (Personal), 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 60.

You can print but choose not to change the host computer’s default printer. This means you will have to explicitly select your printer when you print. To do this, turn off *Make it the default printer on VNC Server* 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 192.168.0.133:1.
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 38. 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 121.
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 37.

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/Linux, VNC Viewer may display a virtual desktop instead, in which case what you see is not the desktop visible to a host computer user. For more information on this feature, see Running multiple instances of VNC Server on page 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 46.

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 45 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 41 for more information. Under Windows, note you can choose for certain other keys or key combinations to be interpreted by your client computer rather than the host. See *Configuring your keyboard* on page 45 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 46.

Note it is possible for client and host computers to have different types of keyboard. Not all the keys available to a host computer user may be available to you, and some keys with the same name may have different behavior. This is especially likely if you are connecting to Mac OS X from Windows or Linux with a PC keyboard, or vice versa; see www.realvnc.com/products/vnc/documentation/latest/misc/keyboard-mapping/.

**Interacting with VNC Server**

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

![VNC Server icon](Windows 7 client computer; Ubuntu 11.10 Linux host)

The VNC Server icon confirms that VNC Server is running on the host computer, provides information to help VNC Viewer users connect, confirms that at least one VNC Viewer user is connected (the icon changes color), and has a shortcut menu to perform useful operations. All this information and functionality is available to you as a connected user. For more information, see *Working with VNC Server on page 81*. 
Chapter 3: Using VNC Viewer

**Note:** Under UNIX/Linux, in some circumstances, the VNC Server icon is not shaded black. Under some versions, no VNC Server icon can be displayed. In the latter scenario, shortcut menu commands are available from the More button on the VNC Server dialog.

Note that the VNC Server icon also provides access to VNC Server options. However, you cannot configure VNC Server in Service Mode unless you know the credentials of a user with administrative privileges on the host computer (or are logged in as one). For more information, see Using the VNC Server - Options dialog on page 88.

### 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 44.

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.

<table>
<thead>
<tr>
<th>Button</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="New Connection" /></td>
<td>Establish a new connection to the same host computer, or to a different one. See Connecting to a host computer on page 37.</td>
</tr>
<tr>
<td><img src="image" alt="Save Connection" /></td>
<td>Save the current connection so you can quickly reconnect without having to remember the network address and authentication credentials. See Appendix A, Saving Connections on page 121.</td>
</tr>
<tr>
<td><img src="image" alt="Close Connection" /></td>
<td>Close the current connection (and the VNC Viewer window).</td>
</tr>
<tr>
<td><img src="image" alt="Options" /></td>
<td>Configure most aspects of VNC Viewer while the current connection is in progress. See Using the VNC Viewer - Options dialog on page 42. Note that some options must be configured before you connect. See Configuring VNC Viewer before you connect on page 35.</td>
</tr>
<tr>
<td><img src="image" alt="Full Screen Mode" /></td>
<td>Toggle full screen mode on and off.</td>
</tr>
<tr>
<td><img src="image" alt="Send Ctrl-Alt-Del" /></td>
<td>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.</td>
</tr>
<tr>
<td><img src="image" alt="File Transfer" /></td>
<td>Browse to the location of client computer files to send to the host computer. See Transferring files between client and host computers on page 62.</td>
</tr>
</tbody>
</table>
Chapter 3: Using VNC Viewer

Using the shortcut menu

VNC Viewer has a shortcut menu that facilitates many of the same common operations as the VNC Viewer toolbar. 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 44.

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

<table>
<thead>
<tr>
<th>Button</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot; ☁ &quot;</td>
<td>Start Chat Session Chat with other VNC Viewer users connected to the same host computer, or with a host computer user. See Communicating securely using chat on page 67.</td>
</tr>
<tr>
<td>&quot; ⌁ &quot;</td>
<td>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.</td>
</tr>
<tr>
<td>&quot; 🎮 &quot; connection speed</td>
<td>Hover over to reveal the current connection speed. For more information on performance, see Changing appearance and behavior on page 44.</td>
</tr>
</tbody>
</table>

(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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relative Pointer Motion</td>
<td>Turn on if the host computer’s mouse cursor appears to be behaving abnormally, for example by accelerating too fast.</td>
</tr>
<tr>
<td>Send F8</td>
<td>Send an F8 command to the host computer. (By default, F8 opens the shortcut menu; see Changing the shortcut menu key on page 46 for how to choose a different key.)</td>
</tr>
<tr>
<td>Ctrl key</td>
<td>Turn on to simulate holding down the CTRL key.</td>
</tr>
<tr>
<td>Alt key</td>
<td>Turn on to simulate holding down the ALT key.</td>
</tr>
<tr>
<td>Refresh Screen</td>
<td>Refresh the display of the host computer’s desktop.</td>
</tr>
<tr>
<td>About VNC Viewer</td>
<td>Display version information. You may need this if you contact Technical Support.</td>
</tr>
</tbody>
</table>

**Using the VNC Viewer - Options dialog**

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

![VNC Viewer - Options](image)

(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 35.
To open the VNC Viewer - 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 44.)

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 121.

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 37.

By default, any options you configure are inherited by the new connection. To prevent this, open the VNC Viewer - 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.
Chapter 3: Using VNC Viewer

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 VNC Viewer - 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 in the expected way.

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 only.

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

Affected keys/combinations: WINDOWS (also known as START), PRINT SCREEN, ALT-TAB, ALT-ESCAPE, CTRL-ESCAPE.
Chapter 3: Using VNC Viewer

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 (Enterprise) and VNC Server (Personal), 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: VNC Server may have been configured to prevent some or all of these features. For more information, see Restricting functionality for connected users on page 93. In addition, VNC Viewer might have been configured to disable printing before the connection started.
You can restrict access to features while the connection is in progress by configuring options on the **Inputs** tab of the **VNC Viewer - 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.

![VNC Viewer - Options dialog](image)

**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 44.

### Making VNC Viewer ‘view only’

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

### Disabling your keyboard

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

### Disabling your mouse

You can disable the client computer’s mouse. To do this, turn off **Enable mouse input**.
Disabling file transfer
You can disable file transfer between client and host computers. To do this, turn off Enable file transfer. For more information about this feature, see Transferring files between client and host computers on page 62.

Disabling copy and paste 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 66.

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 67.
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 to download VNC Viewer for Java from VNC Server (Enterprise) or VNC Server (Personal) on demand; you do not have to install any software. This may be useful if you are at an Internet café, for example.

**Note:** You cannot download VNC Viewer for Java from VNC Server (Free).

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 50
The VNC Viewer for Java user experience 54
Working with VNC Viewer for Java 55
Connecting to a host computer

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

1. Download VNC Viewer for Java from VNC Server (Enterprise) or VNC Server (Personal) running on the host computer you want to connect to. See Downloading VNC Viewer for Java on page 50.

2. Use the VNC Viewer for Java applet to connect to VNC Server. See Connecting to VNC Server on page 52.

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 \texttt{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 \texttt{http://192.168.0.133:5800}.

   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 \textbf{Get Started} section of the \textbf{VNC Server} dialog. More on this dialog.

   \begin{center}
   \includegraphics[width=0.5\textwidth]{get_started.png}
   \end{center}

   \textbf{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 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 8. 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):

```
VNC Server: 192.168.0.133.0
Encryption: Let VNC Server choose
```

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 53.

3. Click the Connect button.

You may be asked to confirm a signature that uniquely identifies VNC Server, acknowledge the encryption status, and to 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 54.

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 VNC Viewer - Options dialog on page 56.

To configure VNC Viewer for Java before you connect, click the Options button in the VNC Viewer dialog. The VNC Viewer - 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.
Chapter 4: Connecting From A Web Browser

The VNC Viewer for Java user experience

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

A. Desktop of a client computer running Windows 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 39.
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):

<table>
<thead>
<tr>
<th>Option</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exit VNC Viewer</td>
<td>Close the current connection (and the VNC Viewer for Java window).</td>
</tr>
<tr>
<td>Clipboard</td>
<td>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 Copying and pasting text on page 57. Note that if you chose not to trust VNC Viewer for Java when you downloaded it, you can only copy and paste text between the two computers via this dialog.</td>
</tr>
<tr>
<td>Send F8</td>
<td>Send an F8 command to the host computer. (F8 opens the shortcut menu.)</td>
</tr>
<tr>
<td>Send Ctrl-Alt-Del</td>
<td>Send the CTRL-ALT-DELETE command to the host computer. (Pressing this key combination would be interpreted by the client computer.)</td>
</tr>
</tbody>
</table>
Chapter 4: Connecting From A Web Browser

Using the VNC Viewer - Options dialog

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh screen</td>
<td>Refresh the display of the host computer’s desktop.</td>
</tr>
<tr>
<td>New connection</td>
<td>Start a new connection to the same host computer, or to a different one, using the same web browser session. You do not need to download VNC Viewer for Java again.</td>
</tr>
<tr>
<td>Options</td>
<td>Configure most aspects of VNC Viewer for Java while the current connection is in progress. See Using the VNC Viewer - Options dialog on page 56. Note that some options must be configured before you connect. See Configuring VNC Viewer for Java before you connect on page 53.</td>
</tr>
<tr>
<td>Connection info</td>
<td>Display technical information about the current connection, such as the encryption method and compression format. You may need this if you contact Technical Support.</td>
</tr>
<tr>
<td>About VNC Viewer</td>
<td>Display information about VNC Viewer for Java. You may need this if you contact Technical Support.</td>
</tr>
<tr>
<td>Dismiss menu</td>
<td>Close the shortcut menu.</td>
</tr>
</tbody>
</table>

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 57.

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 66 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 VNC Viewer - 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 VNC Viewer - 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.
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 (Free). For a summary, see Connecting to VNC on page 13.

**Contents**

- Printing host computer files to a local printer 60
- Transfering files between client and host computers 62
- Copying and pasting text between client and host computers 66
- Communicating securely using chat 67
Printing host computer files to a local printer

If you are connected to VNC Server (Enterprise) or VNC Server (Personal), 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 60.

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

Disabling and enabling printing

You can disable printing providing you do so before you connect. Open the VNC Viewer - 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 (Enterprise) or VNC Server (Personal)? You cannot print VNC Server (Free) files. For more information, see Connecting to VNC 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 60. 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 60. You will have to close the current connection and then reconnect.

   Note that if another VNC Viewer user connected to the same host computer before you, then their local printer becomes the host computer's default. You cannot change this. You 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 prevent printing? If this is the case and you do not have access to the host computer, you will need to consult your system administrator or a host computer user. If you do have access to the host computer, and sufficient privileges to configure VNC Server, you may be able to allow it again. For more information, see Preventing printing on page 94.

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. Alternatively, you may be able to connect as a different host computer user and use this feature. For more information, see Restricting features for particular connected users on page 114.

10. Has the host computer been configured to prevent printing system-wide? If this is the case and you do not have access to it, you will need to consult your system administrator or a host computer user. If you do have access to the host computer, and sufficient privileges to configure both it and VNC Server, you may be able to allow it again. For more information, see Preventing printing on page 94.
Transfering files between client and host computers

If you are connected to VNC Server (Enterprise) or VNC Server (Personal), you can exchange files with the host computer.

Note: If file transfer fails for any reason, see Troubleshooting file transfer on page 65.

Sending files to a host computer

To send files to a host computer:

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

2. Click the Send files button. The VNC Viewer - 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/Linux)**. The **VNC Server - File Transfer** dialog opens on the host computer:

![VNC Server - File Transfer dialog]

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 **VNC Server - File Transfer** dialog. Note you must have write permissions for the folder you choose. Alternatively, you can ask to be prompted each time.
Chapter 5: Exchanging Information

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 \(^2\) (typically shaded black) and, from the shortcut menu, select File Transfer. More on this icon. The VNC Server - File Transfer dialog opens on the host computer:

   ![VNC Server - File Transfer dialog]

   - There are no active or recent downloads to display.
   - To send files to all connected users, click the Send files button, below.
   - To change where downloaded files are saved on this computer, use the Fetch files to drop-down list, below.

2. Click the Send files button. The VNC Server - Send Files dialog opens.

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

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

![VNC Viewer - File Transfer dialog](image.png)

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 **VNC Viewer - 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 can disable file transfer while the current connection is in progress. To do this, open the **VNC Viewer - Options** dialog and, on the **Inputs** tab, turn off **Enable file transfer**.

*More on this dialog.* The **File Transfer** toolbar button is disabled.

You can enable file transfer again at any time.

**Troubleshooting file transfer**

If file transfer does not work, check the following:

1. Are you connected to **VNC Server (Enterprise)** or **VNC Server (Personal)**? You cannot transfer files to or from **VNC Server (Free)**. For more information, see **Connecting to VNC** 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 65.

4. Has **VNC Server** been configured to prevent file transfer? If this is the case and you do not have access to the host computer, you will need to consult your system administrator or a host computer user. If you
do have access to the host computer, and sufficient privileges to configure VNC Server, you may be able to allow it again. For more information, see Preventing file transfer on page 94.

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. Alternatively, you may be able to connect as a different host computer user and use this feature. For more information, see Restricting features for particular connected users on page 114.

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 67.

Disabling and enabling copy and paste text

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

To do this, open the VNC Viewer - Options dialog and, on the Inputs tab, turn off Share clipboard with VNC Server. More on this dialog.

You can enable copy and paste text 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 66.

2. Has VNC Server been configured to prevent 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 able to allow it again. For more information, see Preventing copy and paste text on page 94.

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. Alternatively, you may be able to connect as a different host computer user and use this feature. For more information, see Restricting features for particular connected users on page 114.

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 (Enterprise) or VNC Server (Personal), 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 69.

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:
Chapter 5: Exchanging Information

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

![VNC Server - Chat dialog](image)

**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 **VNC Server - Chat** dialog opens. Type text in the field at the bottom:

![Chat field](image)

3. Press the ENTER key to send the message:

![Chat message](image)

**Note:** A host computer user is identified by the text *(Local)* appended to the user name.
Chapter 5: Exchanging Information

**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:

![Chat window](image)

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

Chat messages are stored on the host computer for 90 days. To stop recording messages, select **Tools > Options** in the *VNC Server - 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/Linux and Mac OS X, this file is located in the host computer user’s `.vnc` directory (you can configure the location under Windows).

Under UNIX/Linux and Mac OS X, you must first stop *VNC Server*, delete the file, and then restart.

Note that when a *VNC Viewer* user disconnects, messages sent by that user change color in the *VNC Server - Chat* dialog.

**Disabling and enabling chat**

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

To do this, open the *VNC Viewer - 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 *VNC Server - 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 (Enterprise)* or *VNC Server (Personal)*? You cannot chat to *VNC Server (Free)* users. For more information, see **Connecting to VNC** 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.
Chapter 5: Exchanging Information

4. Has VNC Viewer been configured to disable chat? To see how to enable it again, read Disabling and enabling chat on page 69.

5. Has VNC Server been configured to prevent chat? If this is the case and you do not have access to the host computer, you will need to consult your system administrator or a host computer user. If you do have access to the host computer, and sufficient privileges to configure VNC Server, you may be able to allow it again. For more information, see Preventing chat on page 94.

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. Alternatively, you may be able to connect as a different host computer user and use this feature. For more information, see Restricting features for particular connected users on page 114.
Setting Up VNC Server

Once licensed, VNC Server permits 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 multiple instances concurrently, configuring ports, and restricting access to features for connected users. For comprehensive information on security, see Chapter 7, Making Connections Secure on page 97.

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 on your own computer for remote access, some features require a host computer user to be present when the connection is established, and should therefore be avoided.

Contents

Licensing VNC Server 72
Starting VNC Server 73
Running multiple instances of VNC Server 78
Working with VNC Server 81
Configuring ports 88
Notifying when users connect 91
Preventing connections to VNC Server 92
Restricting functionality for connected users 93
Stopping VNC Server 95
Chapter 6: Setting Up VNC Server

Licensing VNC Server

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

For more information on the different types of license available, to compare the remote control features provided by each, and to obtain a permanent or a 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 do this when you download and install VNC Server. You may subsequently do so in order to renew a support and upgrades contract.

1. Open the VNC Server shortcut menu. More on this menu.
3. Follow the instructions. Note you may additionally be prompted to configure VNC Server; see Harmonizing VNC Server on page 72 for more information.

Note: If you do not have access to a graphical user interface when you need to apply a license key, use the vnclicense command line tool instead. For more information, run the command vnclicense -help from the directory in which VNC programs are installed.

Harmonizing VNC Server

When you apply a license key you may additionally be prompted to configure 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 you choose to downgrade to VNC Server (Free), you must turn off encryption and system authentication. If you do not, users cannot connect.

Note that it is possible to run more than one instance of VNC Server on a computer (see Running multiple instances of VNC Server on page 78). If this is the case, you must harmonize all running instances separately. For example, if under UNIX/Linux 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 the licensing wizard of 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 not be able to connect to these instances. Note that administrative privileges may be required to perform this operation if you are not the user who started VNC Server.

Understanding license scope

Under Windows, a VNC Server license key is system-wide. This means it applies to all users with accounts on the 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), this means that VNC Server is always licensed for all users.
Under UNIX/Linux and Mac OS X, however, there is another dimension to license scope. The license to use VNC Server not only applies to all computer users, but additionally limits the number of instances of VNC Server that 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 of these are currently running. See page 80 for more information.

Note you can start a maximum of five instances of VNC Server (Free) on UNIX/Linux and Mac OS X computers. Upgrade the host computer to VNC Server (Enterprise) or VNC Server (Personal) if flexibility is important to you.

## Starting VNC Server

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

**Note:** As soon as VNC Server is licensed and started, users can connect. To delay or prevent connections, see Preventing connections to VNC Server on page 92.

### Windows

VNC Server can start in Service Mode, in User Mode, or both. For more information on these modes, which you might want to use, and why you might want to run more than one instance of VNC Server, see Running multiple instances of VNC Server on page 78.

To start VNC Server:

- In Service Mode, select **RealVNC > VNC Server** from the **Start** menu. Note administrative privileges are required to perform this operation.

  **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 automatically restart when the computer is rebooted.

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

  **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.
Chapter 6: Setting Up VNC Server

The VNC Server dialog opens:

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

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

Click the Hide button to minimize the VNC Server dialog but keep VNC Server running in the background.

To access the dialog again, double-click the VNC Server icon in the Notification area. More on this icon.

To see how to explicitly stop VNC Server, or to learn why VNC Server might stop automatically, read Stopping VNC Server on page 95.

UNIX/Linux

VNC Server can start in User Mode, in Virtual Mode, or both, as many times as your license permits. For more information on these modes, which you might want to use, and why you might want to run more than one instance of VNC Server, see Running multiple instances of VNC Server on page 78.

Note: VNC Server can also start in Service Mode, as soon as the host computer boots, and irrespective of whether or not a host computer user is logged on. For more information on this mode in this release, visit www.realvnc.com/products/vnc/documentation/latest/misc/reference/vncserver-x11-serviced.

To start VNC Server:

- In User Mode, either:
  - Select Applications > Internet > VNC Server (User Mode) from the menu system, if available.
  - Run the command `vncserver-x11` in a Terminal window, and press the ENTER key. Note you should not do this as a user with administrative privileges.
The **VNC Server** dialog opens:

![VNC Server dialog](image)

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

Under most versions of UNIX and Linux, you can click the **Hide** button to minimize the **VNC Server** dialog but keep **VNC Server** in User Mode running in the background. To access the dialog again, click the **VNC Server** icon in the Notification Area. More on this icon.

- In Virtual Mode, run the command `vncserver-virtual` in a Terminal window, and press the ENTER key. Note you should not do this as a user with administrative privileges. A message ending with text similar to the following appears:

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

  This operation starts **VNC Server** in Virtual Mode attached to a virtual desktop, detached from the monitor, and independent of the console. This means that no **VNC Server** icon and **VNC Server** dialog comparable to those found in User Mode can be displayed. To see how to work with **VNC Server** in this mode, read Working with **VNC Server** in Virtual Mode on page 77.

  A virtual desktop is assigned an X Server session number corresponding to the port on which **VNC Server** is listening for connection requests. In the example above, this is session number 1, corresponding to port 5901. For more information on ports, see Configuring ports on page 88.

To see how to explicitly stop **VNC Server**, or to learn why **VNC Server** might stop automatically, read Stopping **VNC Server** on page 95.
Chapter 6: Setting Up VNC Server

Mac OS X

VNC Server can start in Service Mode, in User Mode, or both. In addition, VNC Server can start in User Mode (for different users) as many times as your license permits. For more information on these modes, which you might want to use, and why you might want to run more than one instance of VNC Server, see Running multiple instances of VNC Server on page 78.

To start VNC Server:

- In Service Mode, navigate to the Applications > RealVNC folder, and double-click the VNC Server program. Note administrative privileges are required to perform this operation.
  
  **Note:** VNC Server automatically starts when the computer powers on.

- In User Mode, navigate to the Applications > RealVNC > Advanced folder, and double-click the VNC Server (User Mode) program.

The VNC Server dialog opens:

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

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

Click the Hide button to minimize the VNC Server dialog but keep VNC Server running in the background.

To access the dialog again, click the VNC Server icon in the Status bar and, from the shortcut menu, select Open. More on this icon.

To see how to explicitly stop VNC Server, or to learn why VNC Server might stop automatically, read Stopping VNC Server on page 95.
Working with VNC Server in Virtual Mode

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

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

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

- Specify parameters on start-up. See Specifying parameters on start-up on page 77.
- Configure VNC Server as a connected user. See Configuring VNC Server as a connected user on page 77.

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

Specifying parameters on start-up

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

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

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

Parameters specified later in this list override duplicates specified earlier.

For a full list of parameters, run the command vncserver-virtual -list. For more information, run the command man vncserver-virtual.

Configuring VNC Server as a connected user

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

Note: To see how to use VNC Viewer to connect to VNC Server, read Connecting to a host computer on page 37. You will need to qualify the network address of the host computer with the X Server session number assigned when VNC Server starts, for example 192.168.0.187:1.

Under most versions of UNIX/Linux, when you connect, a VNC Server icon is visible to the connected user. For more information on this icon, including how to use it to open the VNC Server dialog and configure VNC Server, start with Using the VNC Server icon on page 81.

Note: If another user connects, the VNC Server icon is shaded black.
Running multiple instances of 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 of VNC Server so that connections to it are optimized for speed, and another so connections are optimized for security. VNC Server facilitates this using modes, each of which permits a different level of access to the host computer.

Note: To see how to start VNC Server in different modes, read Starting VNC Server on page 73.

For more information, read the section appropriate to the platform of the host computer below.

Windows

Under Windows, a host computer user with administrative privileges can start VNC Server in Service Mode. This means VNC Server runs, and users can connect, irrespective of whether or not a host computer user is logged on. By default, in order to connect to:

- VNC Server (Enterprise) or VNC Server (Personal), users must know the user name and password of a member of the Administrators group.
- VNC Server (Free), users must know the VNC password.

In addition, or alternatively, a host computer user can log on and start VNC Server in User Mode. This means VNC Server runs, and users can connect, just while this host computer user is logged on (connections are terminated at log off). By default, in order to connect to:

- VNC Server (Enterprise) or VNC Server (Personal), users must know the user name and password of the currently logged on host computer user.
- VNC Server (Free), users must know the VNC password.

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 Service Mode or User Mode, users have the same privileges (that is, access rights) on the host computer as the currently logged on host computer user. For more information, see Authenticating connections to VNC Server on page 98.

Because only one host computer user can log on to a Windows computer at a time, this means a maximum of two instances of VNC Server can run concurrently on a Windows host computer – one in Service Mode, and one in User Mode for the currently logged on host computer user. Both instances must listen on different ports; see Configuring ports on page 88 for more information.
UNIX/Linux

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

- A VNC Server icon and VNC Server dialog are displayed in order to help the host computer user configure VNC Server after it has started, if necessary.
- Connected users can access applications currently running on the host computer.
- VNC Server stops, and all connections are terminated, when the host computer user starting VNC Server logs off.
- By default, in order to connect to:
  - VNC Server (Enterprise) or VNC Server (Personal), users must know the user name and password of the host computer user starting VNC Server.
  - VNC Server (Free), users must know the VNC password.

Once connected, users have the same privileges (that is, access rights) as this host computer user. For more information on privileges, see Authenticating connections to VNC Server on page 98.

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

- No VNC Server icon or VNC Server dialog can be displayed in order to help the host computer user configure VNC Server after it has started. To see how to work with VNC Server in this mode, read Working with VNC Server in Virtual Mode on page 77.
- Connected users cannot access applications currently running on the console of the host computer. Instead, an isolated workspace is provided. Note this powerful feature can help prevent conflicts; each user can be directed to connect to their own instance of VNC Server in Virtual Mode, and control a (virtual) desktop independently.
- VNC Server does not stop when the host computer user logs off. Users stay connected, and new users can connect. VNC Server must be explicitly stopped.
- By default, in order to connect to:
  - VNC Server (Enterprise) or VNC Server (Personal), users must know the user name and password of the host computer user starting VNC Server.
  - VNC Server (Free), users must know the VNC password.

Once connected, users have the same privileges (that is, access rights) as this host computer user. For more information on privileges, see Authenticating connections to VNC Server on page 98.

Under UNIX/Linux, more than one host computer user can log on at a time. Each currently logged on host computer user can start VNC Server in either mode, and all instances, for all users, run concurrently. Note that all instances must listen on different ports; see Configuring ports on page 88 for more information.
**Chapter 6: Setting Up VNC Server**

_VNC Server_ can run as many times as your license permits. Each time a host computer user starts _VNC Server_ (in either mode), the count of remaining desktops (that is, instances of _VNC Server_) is decremented. To see how many desktops are left, run the command `vnclicense -check`. For example, the output:

<table>
<thead>
<tr>
<th>Licensed desktops:</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running desktops:</td>
<td>3</td>
</tr>
<tr>
<td>johndoe:</td>
<td>2</td>
</tr>
<tr>
<td>janedoe:</td>
<td>1</td>
</tr>
</tbody>
</table>

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

**Note:** You can release licenses by killing desktops. To see how to do this, read _Stopping VNC Server_ on page 95.

**Mac OS X**

Under Mac OS X, a user with administrative privileges can start _VNC Server_ in Service Mode. This means _VNC Server_ runs, and users can connect, irrespective of whether or not a host computer user is logged on. By default, in order to connect to:

- _VNC Server (Enterprise)_ or _VNC Server (Personal)_ users must know the user name and password of a member of the admin group.
- _VNC Server (Free)_ users must know the VNC password.

Once connected, users have the same privileges (that is, access rights) as the currently logged on host computer user. For more information on privileges, see _Authenticating connections to VNC Server_ on page 98.

Depending on the terms of your license, a host computer user can also, or alternatively, log on and start _VNC Server_ in User Mode. This means _VNC Server_ runs, and users can connect, just while this host computer user is logged on (connections are terminated at log off). By default, in order to connect to:

- _VNC Server (Enterprise)_ or _VNC Server (Personal)_ users must know the user name and password of the host computer user starting _VNC Server_.
- _VNC Server (Free)_ users must know the VNC password.

Once connected, users have the same privileges (that is, access rights) as this host computer user. For more information on privileges, see _Authenticating connections to VNC Server_ on page 98.

Under Mac OS X, providing Fast User Switching is turned on, more than one host computer user can log on at a time. Each currently logged on host computer user can start _VNC Server_ in User Mode, and all instances, for all users, run concurrently. Note that all instances, in either mode, must listen on different ports; see _Configuring ports_ on page 88 for more information.

_VNC Server_ can run as many times as your license permits. Each time _VNC Server_ is started, the count of remaining desktops (that is, instances of _VNC Server_) is decremented. To see how many desktops are left, run the command `/Library/VNC/vnclicense -check` in a Terminal window. For more information on the message that is displayed, see the UNIX and Linux section above.
Working with VNC Server

This section explains basic VNC Server features and operations.

Note: For VNC Server in Virtual Mode (UNIX/Linux only), the desktop artifacts explained in this section (icons, menus, and dialog boxes) are available only to a connected user. For more information, see Working with VNC Server in Virtual Mode on page 77.

Using the VNC Server icon

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

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

  ![VNC Server icon on Windows](image)

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

- Under UNIX/Linux, in the Notification Area:

  ![VNC Server icon on UNIX/Linux](image)

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

- Under Mac OS X, on the Status Bar:

  ![VNC Server icon on Mac OS X](image)

The VNC Server icon:

- Provides visual confirmation that VNC Server is running on the host computer. If the icon is not available, then typically VNC Server is not running.

- Provides visual confirmation that VNC Server is configured correctly on the host computer. If not, a red error glyph appears. Open the VNC Server 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:
Using the VNC Server shortcut menu

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

(Note menu options are disabled if they are not applicable.)

**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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>Operate VNC Server. See Using the VNC Server dialog on page 83.</td>
</tr>
<tr>
<td>Information Center</td>
<td>Understand and resolve issues affecting VNC Server, and retrieve system diagnostics. See Using the VNC Server - Information Center dialog on page 87.</td>
</tr>
<tr>
<td>Options</td>
<td>Configure VNC Server. Note administrative privileges are required to perform this operation. See Using the VNC Server - Options dialog on page 88.</td>
</tr>
<tr>
<td>Connections</td>
<td>Identify connected users. See Identifying connected users on page 86.</td>
</tr>
<tr>
<td>About</td>
<td>See version and trademark information, and access a list of open source dependencies.</td>
</tr>
<tr>
<td>Connect to Listening VNC Viewer</td>
<td>Establish a reverse connection in conjunction with a client computer user. See Establishing a reverse connection on page 107.</td>
</tr>
<tr>
<td>Disconnect VNC Viewers</td>
<td>Disconnect all users. Note that, by default, users can immediately reconnect.</td>
</tr>
<tr>
<td>Guest Login</td>
<td>When turned on, and providing VNC Server is configured correctly, a Guest is allowed to connect, bypassing VNC Server’s authentication mechanism. See Allowing a Guest to connect on page 108. Not available in VNC Server (Free).</td>
</tr>
</tbody>
</table>
The **VNC Server** dialog is the gateway to VNC Server, and the first port of call for connection information and troubleshooting:

<table>
<thead>
<tr>
<th>Option</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chat</td>
<td>Chat with all connected users. See <em>Communicating securely using chat</em> on page 67. Not available in VNC Server (Free).</td>
</tr>
<tr>
<td>File Transfer</td>
<td>Send files to all connected users. See <em>Transferring files between client and host computers</em> on page 62. Not available in VNC Server (Free).</td>
</tr>
<tr>
<td>Licensing</td>
<td>Apply a license key to VNC Server. See <em>Licensing VNC Server</em> on page 72.</td>
</tr>
<tr>
<td>Stop VNC Server</td>
<td>Stop VNC Server, disconnecting all users. Note administrative privileges are required to perform this operation. See also <em>Stopping VNC Server</em> on page 95.</td>
</tr>
</tbody>
</table>

To open the **VNC Server** dialog, click its taskbar entry in the normal way for a program, or alternatively 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 84.
- Reveals whether VNC Server is ready to accept connections. See *Troubleshooting VNC Server* on page 84.
- Provides information to help users connect. Start with *Getting users connected* on page 84.
- Displays the VNC Server signature. See *Uniquely identifying VNC Server* on page 86.
Chapter 6: Setting Up VNC Server

- Identifies any connected users. See Identifying connected users on page 86.
- Shows expiry dates for trials or support and upgrades 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:

![VNC Server - Enterprise - Service Mode](image)

You can apply a license key at any time. See Licensing VNC Server on page 72 for more information.

For more information on modes, start with Running multiple instances of VNC Server on page 78.

**Troubleshooting VNC Server**

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

- ✔ Ready for connections

Note there may be messages to read:

- ✔ There is 1 message Show...

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:

- ! There is 1 warning Show...

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:

- ✗ There is 1 problem Show...

An error must be fixed before users can connect.

To read messages, and resolve warnings and errors, click the Show button to open the VNC Server - Information Center dialog, and follow the instructions. *More on this dialog.*

**Getting users connected**

The Get Started section identifies VNC Server running on the host computer over a private network. (For equivalent information for Internet connections, see Connecting over the Internet on page 28.) You can right-click to copy and paste information into an email or similar to help prospective users quickly get connected.
Chapter 6: Setting Up VNC Server

For example:

In this picture, VNC Server is running on a host computer with a private network address of 192.168.0.133. 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 192.168.0.133::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 (Enterprise) or VNC Server (Personal) is serving VNC Viewer for Java on port 5880.

For more information on ports, start with Configuring ports on page 88.

Listing all connectivity options

The Connectivity section lists all network addresses and other means of identifying 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 displayed.
- Four IPv6 network addresses are displayed. 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.)
Chapter 6: Setting Up VNC Server

Uniquely identifying VNC Server

For VNC Server (Enterprise) and VNC Server (Personal), the Get Started section displays a signature uniquely identifying VNC Server:

When a user connects to VNC Server for the first time, that person is asked to verify this signature. For more information on this security feature, see Uniquely identifying VNC Server on page 118.

Identifying connected users

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

Click the Details button to identify and manage connected users. The VNC Server - Connections dialog opens:

In this example, the user of client computer 192.168.0.168:

- Authenticated to VNC Server using the credentials of johndoe. For more information on authentication, start with Authenticating connections to VNC Server on page 98.
- Has a Full set of VNC permissions, permitting unrestricted access to supported RealVNC remote control features while the connection is in progress. For more information, see Restricting features for particular connected users on page 114.

Click the Disconnect button to disconnect a selected user.
Chapter 6: Setting Up VNC Server

Showing expiry dates

The Details section reveals expiry dates for VNC Server (Enterprise) or VNC Server (Personal):

- If you are trialling VNC Server, you are informed of the date on which your trial expires.
- If you have purchased VNC Server, you are informed of the date on which your support and upgrades contract expires.

Using the VNC Server - Information Center dialog

The VNC Server - Information Center dialog enables you to:

- Repair VNC Server. On the Issues tab, follow the instructions for each issue.
- Get system diagnostics in preparation for sending 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.

To open the VNC Server - Information Center dialog, either:

- Select Information Center from the VNC Server shortcut menu. More on this menu.
- Click the Show button when it appears on the VNC Server dialog status bar. More on this dialog.
Chapter 6: Setting Up VNC Server

Using the VNC Server - Options dialog

The VNC Server - Options dialog enables you to configure VNC Server:

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

To open the VNC Server - Options dialog, select Options from the VNC Server shortcut menu. More on this menu. Note under Windows and Mac OS X, administrative privileges are required to perform this operation.

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

For information on most of the options in this dialog, see the subsequent sections in this chapter, starting with Configuring ports on page 88. For more information on the options in the Security area of the Connections tab, and security in general, see Chapter 7, Making Connections Secure on page 97.

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

Configuring ports

By default, VNC Server listens for connections on a particular port. In addition, VNC Server (Enterprise) and VNC Server (Personal) listen for VNC Viewer for Java download requests on a different port. You can change these ports, or make them the same.

Note: VNC Server (Free) does not listen for VNC Viewer for Java download requests. Upgrade the host computer to VNC Server (Enterprise) or VNC Server (Personal) if this feature is important to you.
By default, two separate ports are assigned when VNC Server starts, one for connections and one for download requests:

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

Note: For more information about running multiple instances of VNC Server, and the different modes, see Running multiple instances of VNC Server on page 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 connections and download requests; see Making the connection and download port the same on page 90 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 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 connections and for 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 tab of the VNC Server - Options dialog. More on this dialog.
Chapter 6: Setting Up VNC Server

Changing the connection port
You can change the port on which VNC Server is listening for 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 Accept connections on port field. Note that changing this option does not affect currently connected users.

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

- Web browser users need to know the new port number in order to download. For more information, see Qualifying a network address with a port number on page 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 Serve Java viewer on port field. Note that changing these options does not affect currently connected users.

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

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

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

![Notification Message]

**Note:** A similar message appears on disconnection.

You can choose different notification options on the **Connections** tab of the **VNC Server - Options** dialog. More on this dialog.

Preventing notification messages

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

Displaying connection prompts

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

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

Alternatively, you can **conditionally** replace messages with connection prompts so that they only appear when a host computer user is 'present' to accept or reject them. To do this, choose **Show prompt only if user logged on** (Service Mode) or **Show prompt only if user connected** (Virtual Mode). For more information, see **Preventing particular users connecting** on page 113.
Preventing connections to VNC Server

By default, as soon as VNC Server starts:

- Users can connect to VNC Server and begin controlling the host computer.
- Web browser users can download VNC Viewer for Java from VNC Server (Enterprise) or VNC Server (Personal), and use it to connect.

You can prevent all connection activity by configuring options on the Connections tab of the VNC Server - Options dialog. More on this dialog.

Note: You can alternatively prevent particular users connecting, or connections from particular client computers. See Preventing particular connections to VNC Server on page 111 for more information.

Preventing all connections

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

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

You can still use VNC Server to establish a reverse connection to a client computer. For more information, see Establishing a reverse connection on page 107.

Preventing all VNC Viewer for Java downloads

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

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

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

In addition, for connections to VNC Server (Enterprise) and VNC Server (Personal), users can:

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

You can restrict access to RealVNC remote control features for all connected users, if necessary, by configuring options on the Inputs tab of the VNC Server - Options dialog. More on this dialog.

![VNC Server - Options dialog](image)

Note: In some circumstances, you can restrict access to features for particular users by revoking VNC permissions. See Restricting features for particular connected users on page 114 for more information.

Making VNC Server ‘view only’

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

Disabling the keyboards of client computers

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

Preventing printing
For VNC Server (Enterprise) and VNC Server (Personal), you can prevent all connected users printing host computer files to local printers. To do this, turn off Allow VNC Viewers to share printers. Note this option is on the Printing tab. For more information about this feature, see Printing host computer files to a local printer on page 60.

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

Under Windows, if you have sufficient privileges on the host computer, you can disable printing system-wide by re-installing VNC Server without the VNC Printer Driver component. To do this, turn off VNC Printer Driver at the appropriate step in the Installation Wizard. For more information on installation, visit www.realvnc.com/products/vnc/documentation/latest/installing-removing/windows. The Printing tab is disabled.

Preventing file transfer
For VNC Server (Enterprise) and VNC Server (Personal), you can prevent all connected users exchanging files with the host computer. To do this, turn off Share files with VNC Viewers. For more information about this feature, see Transferring files between client and host computers on page 62.

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

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

Preventing chat
For VNC Server (Enterprise) and VNC Server (Personal), you can prevent connected users communicating securely using chat. To do this, turn off Enable chat. For more information about this feature, see Communicating securely using chat on page 67.
Stopping VNC Server

VNC Server runs until it is stopped.

To explicitly stop VNC Server:

- In all modes and under all platforms except Virtual Mode on UNIX/Linux, select Stop VNC Server from the VNC Server shortcut menu. More on this menu. Administrative privileges are required to perform this operation.
  
  **Note:** Under Windows, VNC Server in Service Mode will not automatically restart if you do so and then reboot the host computer.

- To stop VNC Server in Virtual Mode, run the command `vncserver -kill :x`, where `x` is the X Server session number. For more information, see page 75.

Note that VNC Server automatically stops:

- In Service Mode (Windows and Mac OS X) and in Virtual Mode (UNIX/Linux), when the host computer is powered down.
- In User Mode (all platforms), when the host computer starting it logs off or the host computer is powered down.

VNC Server can also stop under the following circumstances:

- Under Windows, VNC Server in User Mode stops automatically when the last user disconnects if the When last VNC Viewer disconnects option is changed to Logoff user. For more information, see Protecting the host computer on page 119.

- A connected user can explicitly stop VNC Server if they know the credentials of an administrative user.

- 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 73.
Making Connections Secure

VNC Server (Enterprise) and VNC Server (Personal) are designed to permit authenticated and encrypted connections between a host and any number of client computers 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 (Enterprise) if required.

Note: VNC Server (Free) can only authenticate connections. Upgrade the host computer to VNC Server (Enterprise) or VNC Server (Personal) if security is important to you.

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

Contents

Authenticating connections to VNC Server .................................................. 98
Relaxing the authentication rules ................................................................. 104
Bypassing the authentication rules .............................................................. 107
Changing the encryption rules .................................................................... 109
Preventing particular connections to VNC Server ....................................... 111
Restricting features for particular connected users ..................................... 114
Uniquely identifying VNC Server ............................................................... 118
Protecting privacy ......................................................................................... 118
Chapter 7: Making Connections Secure

Authenticating connections to VNC Server

By default, users must authenticate in order to connect to VNC Server. Note this is not the same as logging on to the host computer (though the same credentials may be used for both).

By default:

- VNC Server (Enterprise) and VNC Server (Personal) specify system authentication. This means that a user must supply the credentials of a host computer user in order to connect. See Authenticating using host computer user credentials on page 98.

- VNC Server (Free) specifies VNC authentication. This means that a user must supply a password specific to VNC in order to connect. See Authenticating using a VNC password on page 103.

You can relax the authentication rules, or allow particular users to bypass them altogether, if you consider it safe to do so. For more information, start with Relaxing the authentication rules on page 104.

Authenticating using host computer user credentials

By default, VNC Server (Enterprise) and VNC Server (Personal) specify system authentication, which means that VNC Server is integrated into the credentialing system of the host computer. This mechanism 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 on the host computer can authenticate using already-familiar credentials.

Note: VNC Server (Free) does not support system authentication. Upgrade the host computer to VNC Server (Enterprise) or VNC Server (Personal) if security is important to you.

Note that in some circumstances, the primary user account on the host computer might not have a password set (likely for friends and family only). If so, the authentication mechanism must be changed to VNC authentication, or turned off altogether. A user cannot specify a blank password in order to connect.

By default, the user name and password of a host computer user with administrative privileges must be published to prospective users. Once connected, users:

- Acquire a set of privileges (that is, access rights) on the host computer enabling particular operations to be performed. Note this is not necessarily administrative privileges, even if the credentials of such a user were entered in order to connect.
- Are granted a Full set of VNC permissions, permitting access to all RealVNC remote control features while the connection is in progress.

You can configure VNC Server in order to publish the credentials of a non-administrative host computer user if you wish to either obscure administrator credentials, restrict VNC permissions, or both. Consult the section appropriate to the operating system of the host computer below for more information.
Chapter 7: Making Connections Secure

Windows

Under Windows, system authentication is selected using the Windows password option in the Authentication dropdown of the VNC Server - Options dialog. More on this dialog.

By default, to connect to VNC Server:

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

You can add different users or groups to the authentication list if you do not want to publish the credentials of members of the Administrators group. For more information, see Managing users and groups in the authentication list on page 102.

Note that the credentials supplied by a user in order to connect to VNC Server determine the VNC permissions granted to that user. VNC permissions control which RealVNC remote control features the user is allowed to use. By default, a Full set of VNC permissions is granted. For more information on what this means, and how to revoke VNC permissions in order to restrict access to RealVNC remote control features, see Restricting features for particular connected users on page 114.

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

Under UNIX/Linux, system authentication is selected using the UNIX password option in the Authentication dropdown of the VNC Server - Options dialog. More on this dialog.

This means, to connect to VNC Server in either User Mode or Virtual Mode, a user must supply the credentials of the host computer user starting VNC Server. You can add different users or groups to the authentication list if you do not want to publish the credentials of this host computer user. For more information, see Managing users and groups in the authentication list on page 102.

Note that the credentials supplied by a user in order to connect to VNC Server determine the VNC permissions granted to that user. VNC permissions control which RealVNC remote control features the user is allowed to use. By default, a Full set of VNC permissions is granted. For more information on what this means, and how to revoke VNC permissions in order to restrict access to RealVNC remote control features, see Restricting features for particular connected users on page 114.

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

Under Mac OS X, system authentication is selected using the Mac password option in the Authentication dropdown of the VNC Server - Options dialog. More on this dialog.

This means, to connect to VNC Server:

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

You can add different users or groups to the authentication list if you do not want to publish the credentials of host computer users with administrative privileges. For more information, see Managing users and groups in the authentication list on page 102.

Note that the credentials supplied by a user in order to connect to VNC Server determine the VNC permissions granted to that user. VNC permissions control which RealVNC remote control features the user is allowed to use. By default, a Full set of VNC permissions is granted. For more information on what this means, and how to revoke VNC permissions in order to restrict access to RealVNC remote control features, see Restricting features for particular connected users on page 114.

Once connected to VNC Server:

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

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

By default, VNC Server (Enterprise) and VNC Server (Personal) specify system authentication, which means that a user must supply the credentials of a host computer user in order to connect to VNC Server. Under certain circumstances, this may be the credentials of a host computer user with administrative privileges.

If you want to use system authentication but do not want to publish the credentials of host computer users with administrative privileges, you can add host computer users or groups with less sensitive credentials to the VNC Server authentication list. (Alternatively, you could just choose a different authentication mechanism; for more information, see Relaxing the authentication rules on page 104.)

To manage users and groups in the authentication list, open the VNC Server - Options dialog. More on this dialog. On the Connections tab, click the Configure button. Providing Windows password (or platform-specific equivalent) is selected in the Authentication dropdown, the Permissions for VNC Server dialog opens:

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

Note: Artifacts in this dialog have slightly different names under UNIX/Linux and Mac OS X.

Note that when you add a new host computer user or group to the authentication list, a Default set of VNC permissions is granted to connecting users supplying those credentials, even if this host computer user or group
group has administrative privileges on the host computer. For more information on VNC permissions, see Restricting features for particular connected users on page 114.

Authenticating using a VNC password

By default, VNC Server (Free) specifies VNC authentication, which means that VNC Server has its own password, disassociated from the credentialing system of the host computer. Note this mechanism is only as secure as the complexity of the password chosen.

**Note:** You can specify VNC authentication as the mechanism for VNC Server (Enterprise) or VNC Server (Personal) if you wish.

To enable connections, a VNC Server password must be specified and published to prospective users. Once connected, users acquire a set of privileges (that is, access rights) on the host computer enabling particular operations to be performed. (The same privileges are granted as for system authentication. See Authenticating using host computer user credentials on page 98 for more information.)

VNC authentication is selected using the VNC password option in the Authentication dropdown of the VNC Server - Options dialog. More on this dialog.

To specify a new password, or change an existing one, click the Configure button. The VNC Server - Password dialog opens:
Specify and confirm a password, and click the **OK** button. Publish this password to prospective users, and in addition notify that there is no need to enter a user name in the VNC Viewer **Authentication Credentials** dialog, even if its **Username** field is enabled. *More on this dialog.*

**Specifying additional passwords**

If you choose to use VNC authentication as the mechanism for **VNC Server (Enterprise)** or **VNC Server (Personal)**, you can specify up to two additional passwords, enabling you to differentiate between basic, standard, and power users.  

**Note:** **VNC Server (Free)** does not support additional passwords. Upgrade the host computer to **VNC Server (Enterprise)** or **VNC Server (Personal)** if flexibility is important to you.

Providing the **Extended Configuration** button is enabled, click it to open the **VNC Server - Extended Passwords** dialog:

![VNC Server - Extended Passwords dialog](image)

To give connecting users:

- The power to bypass connection prompts (if enabled), turn on **Enable “Admin” user**, and click the adjacent **Set password** button to specify and confirm an admin password. Publish this password to prospective users, and in addition instruct them to enter a user name of **Admin**. For more information on connection prompts, see *Preventing particular users connecting* on page 113.

- View only access to the host computer, turn on **Enable “ViewOnly” user** and click the adjacent **Set password** button to specify and confirm a view only password. Publish this password to prospective users, and in addition instruct them to enter a user name of **ViewOnly**.

**Relaxing the authentication rules**

You can relax the authentication rules for all prospective users if you consider it safe to do so. For more information on the default authentication mechanisms, see *Authenticating connections to VNC Server* on page 98.

**Note:** Alternatively, you can allow particular users to bypass authentication altogether. For more information, see *Bypassing the authentication rules* on page 107.

For **VNC Server (Enterprise)**, you can relax the authentication rules so that users:

- Need only enter a VNC password. This forgoes the need to publish host computer user credentials, and for users to have to remember a user name. For more information, see *Authenticating using a VNC password* on page 103.
• Authenticate automatically using the credentials the user has already entered to log on to their client computer. This speeds up the connection process and helps prevent password fatigue. For more information, see Authenticating automatically using client computer user credentials on page 105.

• Do not have to authenticate at all. This may allow older versions of VNC Viewer (or VNC-compatible Viewer technology) that do not support authentication to connect. For more information, see Turning authentication off on page 106.

For VNC Server (Personal), you can relax the authentication rules so that users need only enter a VNC password, or do not have to authenticate at all. For VNC Server (Free), you can only relax the rules so that users do not have to authenticate at all. Upgrade the host computer to VNC Server (Enterprise) if security is important to you.

Authenticating automatically using client computer user credentials

You can configure VNC Server (Enterprise) to authenticate a user automatically using the credentials already entered by that user to log on to their client computer. Note this authentication mechanism is only effective in a managed network environment, with (for example) a Kerberos authentication server.

Note: VNC Server (Free) and VNC Server (Personal) do not support single sign-on. Upgrade the host computer to VNC Server (Enterprise) if security is important to you.

To do this, choose the Single Sign On option in the Authentication dropdown of the VNC Server - Options dialog. More on this dialog.

There is no need to publish credentials to prospective users. Once connected, users:

• Acquire a set of privileges (that is, access rights) on the host computer enabling particular operations to be performed.

• Are granted a set of VNC permissions, permitting access to RealVNC remote control features for the duration of the connection.
Chapter 7: Making Connections Secure

The same privileges and VNC permissions are granted as for system authentication. See Authenticating using host computer user credentials on page 98 for more information.

Turning authentication off

You can turn authentication off for all users. Note you should only do this if you are sure all prospective users are trustworthy.

**Note:** You can allow just particular users to connect without supplying a password. See Bypassing the authentication rules on page 107 for more information.

To do this, choose the None option in the Authentication dropdown of the VNC Server - Options dialog. More on this dialog.

(Note this option is only available when the dialog is in Advanced mode.)

There is no need to publish credentials to prospective users.

Once connected, users acquire a set of privileges (that is, access rights) on the host computer enabling particular operations to be performed. The same privileges are granted as for system authentication. See Authenticating using host computer user credentials on page 98 for more information.
Bypassing the authentication rules

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

**Note:** You can turn authentication off for all users if you consider it safe to do so. For more information, see *Turning authentication off* on page 106.

You can either:

- Establish a reverse connection to a particular client computer. See *Establishing a reverse connection* on page 107.
- Allow a particular user to connect as a Guest. See *Allowing a Guest to connect* on page 108. Note this remote control feature is not available in VNC Server (Free).

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

**Establishing a reverse connection**

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

**Note:** The client computer must be running Listening VNC Viewer. For more information, see *Starting Listening VNC Viewer* on page 34.

Note this feature is also useful if the host computer is protected by a firewall that cannot be configured to allow network communications, 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:

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

   ![VNC Server - Connect to Listening VNC Viewer](image)

   Enter the address of the computer to connect to, which must be running 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 27.

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, see Chapter 3, Using VNC Viewer on page 33.

Allowing a Guest to connect

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

Note: VNC Server (Free) does not support guest connections. Upgrade the host computer to VNC Server (Enterprise) or VNC Server (Personal) if flexibility is important to you.

To enable Guests to connect:

1. Open the VNC Server - Options dialog. More on this dialog. On the Connections tab, select an alternative to the default None option from the Guest access dropdown:

   ![VNC Server - Options dialog]

To give users:

— The ability to remote control the host computer, select Interactive.
— View only access, select View-only. Any keypresses or mouse movements made by the user will have no effect.

2. Turn on the Guest Login option on the VNC Server shortcut menu. More on this menu. A tick appears:

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

3. Inform users that they must enter Guest in the Username field of the VNC Viewer - Authentication dialog. More on this dialog. The Password field, however, should be left empty.

When a Guest connects, a connection prompt appears on the host computer:

A host computer user must accept the connection request within ten seconds or it will be automatically rejected. For more information on connection prompts, see Preventing particular users connecting on page 113.

Changing the encryption rules

By default, all network communications to and from a host computer running VNC Server (Enterprise) or VNC Server (Personal) are encrypted using 128-bit AES technology. Identity is certified using 2048 bit RSA public/private keys.

Note: VNC Server (Free) does not support encryption. Upgrade the host computer to VNC Server (Enterprise) or VNC Server (Personal) if security is important to you.

For VNC Server (Enterprise), 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, passwords are still encrypted.
Chapter 7: Making Connections Secure

- 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 (Personal), you can just relax the encryption rules. 256-bit AES encryption is not available. Upgrade the host computer to VNC Server (Enterprise) if security is important to you.

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

To change the rules, open the VNC Server - Options dialog. More on this dialog. On the Connections tab, select an alternative to the default Always on option from the Encryption dropdown:

![VNC Server - Options 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 reduced to 128-bit.

- **Prefer on** to prefer, though not mandate, that connections be encrypted using 128-bit AES. A connecting user can either request 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 particular connections to VNC Server

You can prevent particular users connecting to VNC Server. You can either:

- Prevent connections from particular client computers. See Preventing connections from particular client computers on page 111.
- Prevent particular users connecting. See Preventing particular users connecting on page 113.

Note: You can prevent all users connecting to VNC Server. For more information, see Preventing connections to VNC Server on page 92.

Preventing connections from particular client computers

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

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

To filter network addresses, open the VNC Server - Options dialog. More on this dialog. On the Connections tab, click the IP Filter button:
Chapter 7: Making Connections Secure

By default, connection requests are accepted from all client computers. To reject connection requests from a particular client computer, click the **Add** button:

![VNC Server - Add Rule dialog](image)

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept the connection</td>
<td>Accepts connection requests from the specified client computer(s).</td>
</tr>
<tr>
<td>Reject the connection</td>
<td>Rejects connection requests from the specified client computer(s).</td>
</tr>
<tr>
<td>Ask the VNC Server user what to do</td>
<td>Displays connection prompts enabling a host computer user to either accept connection requests, allow 'view only' access, or reject requests from the specified client computer(s). If no host computer user is present, connection requests are automatically rejected after 10 seconds. For more information on connection prompts, see <em>Preventing particular users connecting</em> on page 113.</td>
</tr>
</tbody>
</table>

Note that if you do filter network addresses, the order of rules in the **VNC Server - Filter Rules** dialog is important. The first matching rule determines what happens to connection requests from a particular client computer. For example, if a rule rejecting a client computer is encountered before one accepting it, then all connection requests from that client computer will be rejected. You can move rules up and down in the dialog using the arrows.

By default, the **Default** rule *accepts* connection requests from all client computers. You can change this so that it rejects or queries all connection requests instead. To do this, select the **Default** rule, and click the **Edit** button. Note this rule is always last in the dialog.
Preventing particular users connecting

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

![Connection Prompt](Image)

A connection prompt enables a host computer user (if one is present), or an already-connected user, to identify the connecting user and either accept the connection request, allow ‘view only’ access to the host computer, or reject it. If no response is received within ten seconds, then the connection request is automatically rejected. Note that if you are setting up VNC Server on your own computer for remote access then enabling this feature may prevent you connecting.

**Note:** In some circumstances, certain users connecting to VNC Server (Enterprise) or VNC Server (Personal) are able to bypass connection prompts. To submit these users to prompts, revoke the Connect without accept/reject prompt VNC permission. For more information, see Customizing VNC permissions on page 115.

To display connection prompts, open the VNC Server - Options dialog. More on this dialog. On the Connections tab, choose Show accept/reject prompt from the When VNC Viewers connect dropdown:
In certain circumstances, you may be able to conditionally display connection prompts:

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

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

For more information on notifications, see Notifying when users connect on page 91.

Restricting features for particular connected users

A set of VNC permissions is granted to each user who connects to VNC Server (Enterprise) or VNC Server (Personal) using either of the following authentication mechanisms:

- System authentication. See Authenticating using host computer user credentials on page 98.
- Single sign-on. See Authenticating automatically using client computer user credentials on page 105.

Note: VNC Server (Free) does not support VNC permissions. Upgrade the host computer to VNC Server (Enterprise) or VNC Server (Personal) if security and flexibility are important to you.

VNC permissions control which RealVNC remote control features a connected user is allowed to use. By default, a user supplying the credentials:

- Of a host computer user with administrative privileges is granted a Full set of VNC permissions.
- Of any other host computer user is granted a Default set of VNC permissions.
The following table explains VNC permissions (and the groups in which they may be allocated):

<table>
<thead>
<tr>
<th>Permission name</th>
<th>When granted, a connected user can...</th>
<th>Full</th>
<th>Default</th>
<th>View Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>View display contents</td>
<td>See the host computer's desktop.</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Send pointer events</td>
<td>Control the host computer using the client computer's mouse.</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Send keyboard events</td>
<td>Control the host computer using the client computer's keyboard.</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Send and receive clipboard contents</td>
<td>Copy and paste text between applications running on the client and host computers.</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Send and receive files</td>
<td>Exchange files with the host computer.</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Add VNC printers</td>
<td>Print host computer files to a local printer.</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Accept chat messages</td>
<td>Chat with other VNC Viewer users, or with a host computer user.</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Connect without accept/reject prompt</td>
<td>Bypass connection prompts. For more information about this feature, see Preventing particular users connecting on page 113.</td>
<td>YES</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Customizing VNC permissions**

You can customize VNC permissions for particular users, perhaps in order to revoke permissions for certain RealVNC remote control features while just those users are connected.

**Note:** You can restrict access to RealVNC remote control features for all connected users by configuring options on the Inputs tab of the VNC Server - Options dialog. For more information, see Restricting functionality for connected users on page 93.
To customize VNC permissions, open the VNC Server - Options dialog. Make sure either Windows password (or platform-specific equivalent) or Single sign-on is selected in the Authentication dropdown on the Connections tab, and click the Configure button:

![Permissions for VNC Server dialog](image)

**Note:** A user can supply the credentials of any of the host computer users listed in Group or user names in order to connect to VNC Server (including any member of a group). To see how to configure host computer users or groups, see Managing users and groups in the authentication list on page 102.

You can change the VNC permissions allocated to a particular host computer user. To do this, select the appropriate entry in the Group or user names list, and turn individual permissions on or off. For example, in
the following dialog, just the **View display contents**, **Send pointer events**, and **Send keyboard events** permissions are turned on for the host computer user Jane Doe:

![Permissions for VNC Server](image)

This means that any user supplying Jane Doe's credentials in order to connect to VNC Server is able to see the host computer's desktop, and control it using their keyboard and mouse. All other RealVNC remote control features, however, are disabled. A user will not be able to copy and paste text, print, chat, transfer files, or bypass connection prompts.
Chapter 7: Making Connections Secure

Uniquely identifying VNC Server

VNC Server (Enterprise) and VNC Server (Personal) have a uniquely identifying signature:

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

**Note:** VNC Server (Free) does not have a unique signature. Upgrade the host computer to VNC Server (Enterprise) or VNC Server (Personal) if security is important to you.

The VNC Server signature is displayed in the Get Started area of the VNC Server dialog. More on this dialog.

![Image of VNC Server signature](image.png)

When a user connects from a particular client computer for the first time, this signature is published. The user is asked to verify that the signature they see matches that of VNC Server. See Checking the signature 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:

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

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

The new VNC Server signature is fa-a5-76-c9-3d-df-ca-1d.

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

then it is recommended that they do not connect.

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

Protecting privacy

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

By default, VNC Server promotes shared connections. That is to say, if more than one user is connected, all users can observe each other’s operations, and if a host computer user is present, then that user can observe the operations of connected users.
Under Windows, you can configure VNC Server to uphold the privacy of connected users by editing various options in the VNC Server - Options dialog. More on this dialog.

Blanking the host computer’s monitor

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

Preventing input from the host computer

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

Protecting the host computer

Note: The information in this section applies to VNC Server in Service Mode only.

You can protect the host computer when no connections are in progress by locking it or logging off when the last user disconnects. To do this, select an alternative to the default Do nothing option from the When last VNC Viewer disconnects dropdown on the Desktop tab:

To protect the host computer by:

- Locking the workstation, select Lock workstation. Users can immediately reconnect, but must know how to unlock the host computer in order to continue. Note that if you apply this setting to VNC Server in User Mode, users can reconnect but see only a non-operational black screen, and cannot continue.
- Logging off, select Logoff user. Users can immediately reconnect, but must know how to log on to the host computer in order to continue.
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, and 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 122
- Using VNC Address Book to connect 127
- Managing connections using VNC Address Book 128
- Saving connections to desktop icons 131
Appendix A: Saving Connections

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 131.

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 130.

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 \(\mathbf{\nabla}\) throughout VNC Address Book.

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

![Enter Master Password]

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

![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 127.

For more information on editing and organizing connections, start with *Organizing connections* on page 129.
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:

![VNC User Guide](image)

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 35.
4. Click the **OK** button. If you chose to create a protected connection, and this is the first time you have used *VNC Address Book*, you are prompted to specify a master password:

![Enter Master Password](image)

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

![VNC Address Book](image)

To see how to use *VNC Address Book* to connect to this host computer, read *Using VNC Address Book to connect* on page 127.

For more information on editing and organizing connections, start with *Organizing connections* on page 129.
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 130.

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 128.
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/Linux, 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, run the command vncaddrbook, and press the ENTER key. Note you should not do this as a user with administrative privileges.

- Under Mac OS X, navigate to the Applications > RealVNC folder, and double-click the VNC Address Book program.

Working with VNC Address Book

Under Windows, while VNC Address Book is running, a VNC Address Book icon is displayed in the Notification area. 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/Linux and Mac OS X, no VNC Address Book icon is available. However, most operations explained below can be performed from the VNC Address Book dialog.

The VNC Address Book icon:

- Provides visual confirmation that VNC Address Book is running on the client computer. If the icon is not available, then VNC Address Book is not running.
Appendix A: Saving Connections

• Has a shortcut menu that performs useful operations:

![Shortcut Menu]

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect to</td>
<td>Choose a host computer to connect to.</td>
</tr>
<tr>
<td>Launch VNC Viewer</td>
<td>Start VNC Viewer, enabling you to connect to a new host computer in the standard way. For more information, see Connecting to a host computer on page 37.</td>
</tr>
<tr>
<td>Open Address Book</td>
<td>Create new connections or edit and organize existing ones. (Alternatively, double-click the VNC Address Book icon to open the VNC Address Book dialog.)</td>
</tr>
<tr>
<td>Exit</td>
<td>Close VNC Address Book.</td>
</tr>
</tbody>
</table>

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.
Appendix A: Saving Connections

For more information on editing VNC Viewer options, start with Configuring VNC Viewer before you connect on page 35.

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 Alphabetic 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 122.

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.
Appendix A: Saving Connections

- **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:

![Desktop Icon](image)

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.