

REAL

**VNC 4**

**Deployment Tool**

**User Guide**



# Contents

<b>Preamble</b>	<b>3</b>	<b>Configuring settings</b>	<b>12</b>
Software Versions	3	Configuring a single host	12
Software Requirements	3	Configuring multiple hosts	13
Compatibility	3	Configuring NtLogon Access Control	15
<b>Introduction</b>	<b>4</b>	Configuring Password Parameters	15
The VNC Deployment Tool window	4	Settings index	16
<b>Scanning</b>	<b>5</b>	Main tab settings	16
Scanning the network	5	Settings from the Security tab	17
Saving and loading scans	6	Settings from the Connections tab	19
Using credentials	6	Settings from the Inputs tab	20
<b>Installing VNC</b>	<b>7</b>	Settings from the Sharing tab	21
Selecting install options	7	Settings from the Desktop tab	22
Installing, reinstalling and uninstalling	8	Settings from the Capture method (Hooks) tab	23
<b>Controlling licences</b>	<b>9</b>	Settings from the Legacy tab	24
Auditing licences	9	Extra settings	25
Upgrading out-of-date licenses	10	Support	26
Reallocating licenses	10	Via the web	26
		By post	26
		<b>Index</b>	<b>27</b>

# Preamble

## Software Versions

This document covers all versions of VNC Deployment Tool from version 1. However, it includes features that are not available in all versions. Where the operation or user interface of the software has changed substantially, this is marked in the text using coloured backgrounds as follows:

The feature described was added in version 1.4, or has changed substantially between versions 1.3 and 1.4.

The feature described was added in version 1.5, or has changed substantially between versions 1.4 and 1.5.

The feature described was added in version 1.6, or has changed substantially between versions 1.5 and 1.6.

## Software Requirements

The VNC Deployment Tool requires Windows NT 4 or later, Windows 2000, Windows XP Professional or Windows 2003 Server to run. The following table summarises the requirements imposed upon remote systems that are to be administered:

### In order to...

Scan hosts using alternative credentials, Install, Uninstall

Scan hosts, Audit licenses, Configure settings

### The remote host must be running...

Windows NT 4 or later, Windows 2000, Windows XP Professional or Windows 2003 Server

Windows 98 with Remote Registry, Windows NT 4 or later, Windows 2000, Windows XP Professional or Windows 2003 Server

## Compatibility

VNC Deployment Tool is compatible with the following versions of VNC software running under the versions of Windows shown opposite:

### Installation and Configuration

All versions of VNC Enterprise Edition.

### Removal

All versions of VNC Enterprise Edition, VNC Personal Edition and VNC Free Edition from RealVNC Ltd; VNC versions 3.3.3–3.3.7 from AT&T Laboratories, Cambridge; TightVNC version 1.2.9 and above; UltraVNC versions 1.01 and 1.02.

### Detection

All known versions of VNC. Specifically, any version of VNC that runs as a service named WinVNC or WinVNC4.

# Introduction

The VNC Deployment Tool provides an invaluable service to administrators who need to manage multiple VNC installations within an organisation. Using the VNC Deployment Tool, you can:

- [Scan part or all of an existing network](#)
- [Start, stop, install, uninstall or update VNC on multiple hosts](#)
- [Check and reallocate license keys](#)
- [Alter and apply configuration settings](#)

## The VNC Deployment Tool window

The main menu items cover the four central functions of the VNC Deployment Tool:

[Scan](#) • [Install](#) • [License key audit](#) • [Configure](#)

The screenshot shows the VNC Deployment Tool window with a menu bar (Scan, Installation, Licenses, Configuration, View, Help) and a tree view of a network. A context menu is open over a host named 'moth'. Callouts point to the main menu, the network view, the detail view, and the popup menu.

Menu Item	Shortcut
Start Scan	Ctrl+T
Save Results...	Ctrl+S
Load Results...	Ctrl+O
Credentials...	Ctrl+K
Options...	F2

Menu Item	Shortcut
Install/Reinstall...	Ctrl+R
Uninstall...	Ctrl+U
Start VNC Service...	
Stop VNC Service...	
Options...	Ctrl+F2

Menu Item	Shortcut
Audit Licenses...	Ctrl+A
Add/Remove Licenses...	Ctrl+L

Menu Item	Shortcut
Import VNC Settings...	Ctrl+I
Export VNC Settings...	Ctrl+X
Quick Configure...	Ctrl+Q
Edit Configuration...	Shift+F2

Menu Item	Shortcut
Import VNC settings	Ctrl+C
Export VNC settings	Ctrl+V
Quick Configure...	
Install/Reinstall	
Uninstall	
Start VNC Service	
Stop VNC Service	
Connect	Ctrl+N
Refresh	F5

**Network view**  
The upper pane provides an overview of the network

**Detail view**  
The lower pane provides details about the selected network item

**Popup menu**  
Numerous functions can be carried out by right clicking on a host, domain or network name.

# Scanning

## Scanning the network

The first step is usually to perform a scan to discover the current layout and status of the network (you can alternatively [load a previously saved scan](#)). By default, the VNC Deployment Tool will search the hosts registered within the Network Neighbourhood, however you can change this using the [Scan Options](#) dialog.

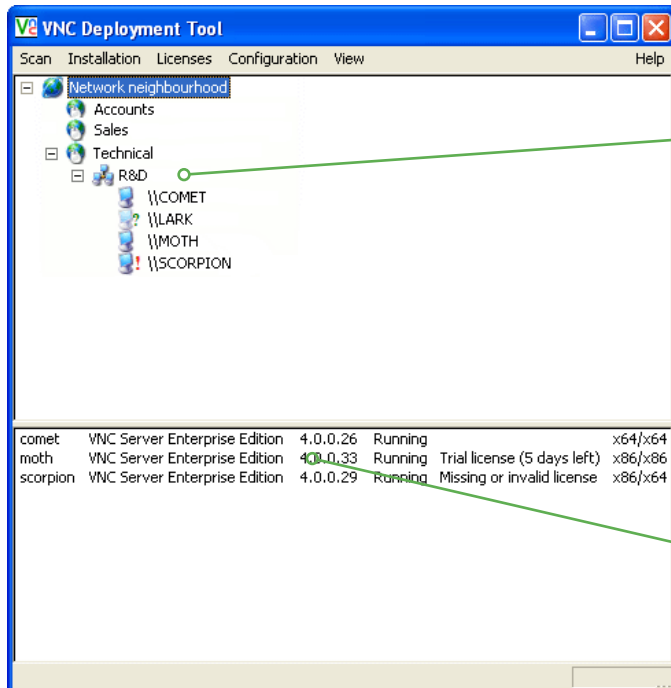
*Note: Ensure that you are logged in as administrator or an alternative high level user with sufficient rights to access other network hosts. See [To add credentials](#) for details about supplementing your standard access rights.*

### To scan the network

- 1 Click the *Scan* menu and select *Start Scan* (keyboard shortcut: CTRL+T).

*Note: The Network Neighbourhood will be scanned by default unless you change the scanning option to 'Entire Network' or define an 'IP address range'—see [To change scanning options](#) for details.*

- 2 As the systems are located, their names and status will be added to the VNC Deployment Tool window:



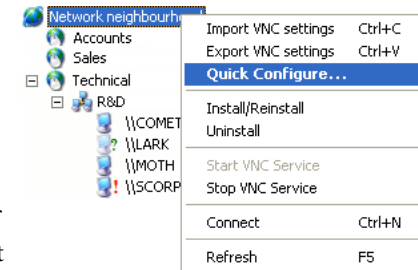
The upper *Network view* pane shows a graphical representation of the scan with named node icons for each network, domain and host system.

The lower *Detail view* pane provides information about items related to the currently highlighted node in the network view pane.

### Key to icons

- Top level node for the Entire Network
- Top level node for the Network Neighbourhood
- A network
- A Windows domain or top level node for an IP address range
- A successfully scanned host
- An unsuccessfully scanned host. Select the host to view details of the problem. Common reasons for failure are: the host is unavailable or not running Windows, or that the VNC Deployment Tool does not have permission to access the host.
- A successfully scanned host that requires attention. The detail view will display an explanation of the type of error encountered, usually an issue with the license key.
- An unknown node. The detail view will display an explanation of the type of error encountered.

Right click on any network, domain or host node to reveal a popup menu with available options.



### Scan details

Clicking on a host in the upper pane of the window displays information about that host in the lower pane. Clicking on a network or a domain node in the upper pane displays information about all successfully-scanned children in the lower pane. This information includes the name of the host; vendor and version information for the VNC installation (if any); the current state of the VNC Service and any licensing problems that require attention.

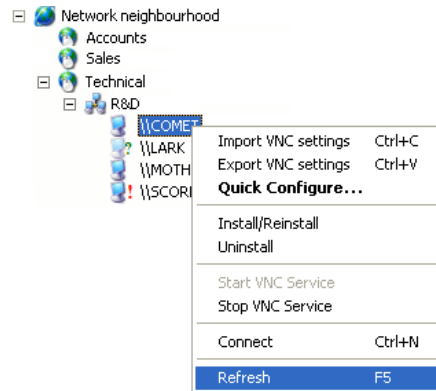
This pane also displays information regarding the processor architecture (x86, x64 or ia64) and the architecture supported by the currently-installed version of VNC (x86 or x64). For example, x86/x64 indicates a 32-bit version of VNC running on an x64 platform. Unrecognised architectures are denoted by a question mark.

## To rescan a single node

In large installations it can be time consuming to rescan the whole network. In cases where only a few hosts or just one domain have changed, it is quicker to rescan only the affected node.

- 1 Right click on the required host or domain node.
- 2 From the subsequent popup menu, select *Refresh* (keyboard shortcut: F5).

The latest status for the selected node will be reflected within the VNC Deployment Tool window.

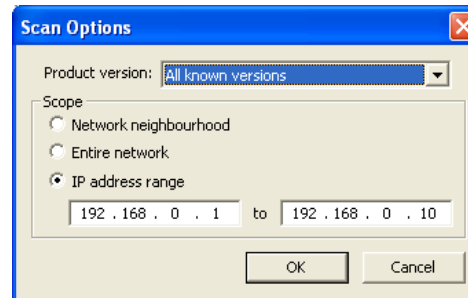


## To change scanning options

- 1 Click the *Scan menu* and select *Options...* (keyboard shortcut: F2).

The *Scan Options* dialog will be displayed:

- 2 Choose the appropriate *Product version* and *Scope* setting:
  - **Network neighbourhood** – searches only the hosts registered in the Network neighbourhood (or My Network) of the system that is running the VNC Tool application.
  - **Entire network** – searches for hosts on the entire local network to which the system running the VNC Tool application belongs.
  - **IP address range** – allows you to define the range within which the VNC Deployment Tool will scan and operate.
- 3 Click the *OK* button to apply the setting.



## Saving and loading scans

The VNC Deployment Tool allows you to save network scans and then reload them at a later date. When a network is relatively stable and unchanging, this option can save time in re-scanning the whole installation whenever the VNC Deployment Tool is used. Individual nodes can then be refreshed by right clicking on them and selecting the *Refresh* option.

### To save network scan results

- 1 Click the *Scan menu* and select *Save Results...* (keyboard shortcut: CTRL+S).
- 2 In the subsequent file dialog, choose a location and define a file name.
- 3 Click the *Save* button.

### To load previous network scan results

- 1 Click the *Scan menu* and select *Load Results...* (keyboard shortcut: CTRL+O).
- 2 In the subsequent file dialog, select the location file name of the required scan results.
- 3 Click the *Open* button.

The saved network layout and status information will be displayed within the two sections of the VNC Deployment Tool window.

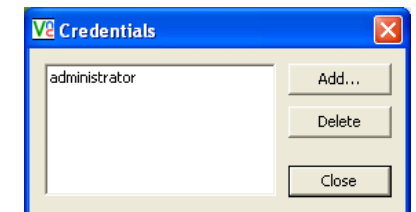
Alternatively, you can load scan results by dragging and dropping the file onto the VNC Deployment Tool window.

## Using credentials

Even when logged-in as the administrator, certain hosts within the network may not allow access until further username and password details are given. The credentials option allows you to store such details so that the VNC Deployment Tool can apply them automatically. When a scan is carried out, your standard login and password will be initially used. If any hosts refuse access at this point, the VNC Deployment Tool will run through the entered credentials list until a successful match is found. Depending on the number of credentials entries, the overall scan time may be increased. You can also use this feature to administer VNC across multiple network domains by using suitable foreign domain accounts.

### To add credentials

- 1 Click the *Scan menu* and select *Credentials...* (keyboard shortcut: CTRL+K).
- The Credentials dialog will be displayed:
- 2 Click the *Add...* button and in the subsequent dialog, enter a suitable *Username* and *Password* that will gain access to one or more hosts.
  - 3 Click the *OK* button and then either click *Close* or add further entries as per step 2.



# Installing VNC

The VNC Deployment Tool allows you to add, remove or update VNC on any or all systems within your network or domain. Hosts can be selected individually, in groups or as part of a complete domain or network.

## Selecting install options

Before using the VNC install/reinstall option it is important to ensure that the Install options are correctly configured as these will have a direct effect on how remote hosts are affected.

### To view/alter install options

- 1 Click the *Installation* menu and select *Options...* (keyboard shortcut: CTRL+F2).

The Install options dialog will be displayed:

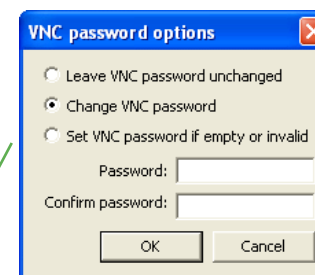
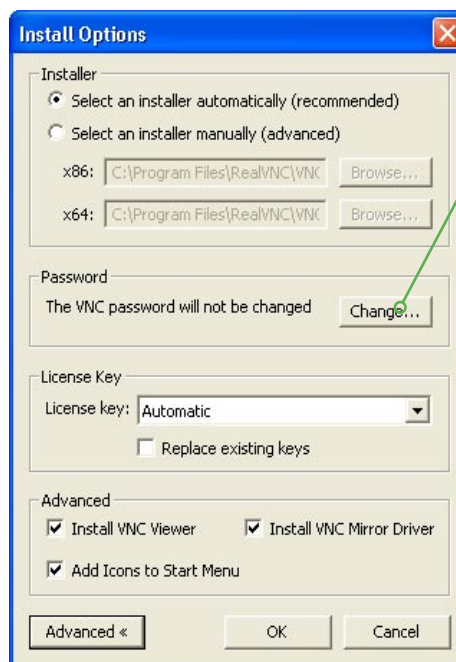
- 2 Alter settings as required and then click the *OK* button.

- **Installer** Determines which installation file will be used for the selected hosts. If **Select an installer automatically (recommended)** is selected, then the VNC Deployment Tool installation directory will be searched for a VNC installer and this will be used if found; this is the default. If **Select an installer manually (advanced)** is selected, then you can provide a different installer; this allows you to install other versions of VNC.

Starting with version 1.6, 64-bit Windows systems are supported (x64 only). If an x64 installer is specified manually, or is placed into the VNC Deployment Tool installation directory, then it will be used for x64 systems. The x86 installer will be used for all other systems, and will be used for all systems if no x64 installer is configured.

If you are installing VNC Enterprise Edition version E4.3 or later, then you do not need to specify separate installers for x86 and x64 systems. Starting with version E4.3, a single installer is used for both x86 and x64 systems.

- **License key** Determines how a license key will be applied to host installation. Options include:
  - **Do not install a license key** Suitable if VNC Free Edition is being installed or license keys will be manually configured at each host or they will be installed later from the VNC Deployment Tool using the [Licenses](#) options.
  - **Automatic** Copies of licenses held within the VNC Deployment Tool will be allocated to selected (un-licensed) hosts, up to the maximum allowable number of copies per license.



- **Individual listed licenses** Any named license in the list can be selected for distribution to hosts, up to the maximum allowable number of copies for that license.
- **Replace existing keys** When ticked, this option will apply the current license key policy even to selected hosts that already possess an existing license key.

- **Password** Click *Change...* to display the VNC Password options dialog. This allows you to determine how the VNC Server password will be configured at each host.

- **Leave VNC Password unchanged** Makes no change to VNC password settings.
- **Change VNC password** Alters the password for all selected hosts to the one entered within this dialog, regardless of their current status.
- **Set VNC password if empty or invalid** Changes the password for all selected hosts, to the one entered within this dialog, only where a valid password does not already exist.

- **Advanced** Controls advanced features of the installation:
  - **Install VNC Viewer** Include the VNC viewer when installing.
  - **Install VNC Mirror Driver** Include the VNC mirror driver when installing. Note that this option has no effect unless you are installing VNC Enterprise Edition version E4.3 or later.
  - **Add Icons to Start Menu** Add the standard VNC icons to the start menu.

[Installing, reinstalling and uninstalling](#) ⇌

# Installing, reinstalling and uninstalling

You can initiate an installation/reinstallation or uninstallation operation in two main ways, either:

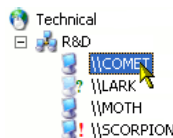
- By selecting host, domain or network nodes in the VNC Deployment Tool window, or
- By naming hosts via the Installation menu.

*Note: The former method is best suited when installing across a whole domain or network.*

## To install/reinstall or uninstall by clicking nodes

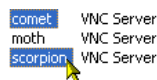
1 In the VNC Deployment Tool window, select the nodes that you wish to affect:

- **Select a node (host, domain or network):** Click on the required node in either the upper or lower panes of the VNC Deployment Tool window.



*Note: If you select a domain or network, the chosen operation will affect all descendants of that domain or network.*

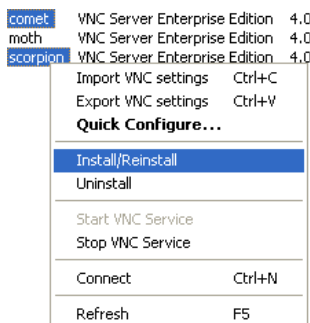
- **Select two or more hosts:** In the lower pane of the VNC Deployment Tool window:
  - Use CTRL and click to select individual host names, or
  - Use SHIFT and click to select a range of hosts.



2 Right click on one of the selected names to reveal a popup menu.

3 Select the required option:

- **Install/Reinstall:** Install or update VNC on the selected node(s) using the VNC installer version selected in the [Install options](#) dialog.



- **Uninstall:** Remove VNC from the selected node(s).

*Note: The uninstall feature is not available for all VNC versions.*

4 A message will be displayed upon completion of the chosen task. If problems were encountered with any hosts, then details will be shown in the lower pane.

## To install/reinstall or uninstall using the Installation menu

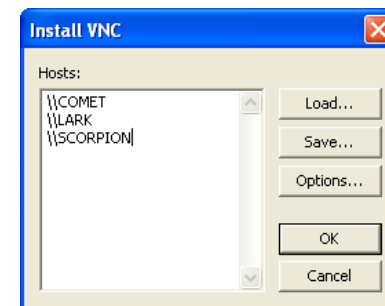
1 Click the *Installation* menu and select the required option:

- **Install/Reinstall:** Install or update VNC on the selected node(s) using the VNC installer version selected in the [Install options](#) dialog.
- **Uninstall:** Remove VNC from the selected node(s).

Depending on the option selected, either the *Install VNC* or *Uninstall VNC* dialog will be displayed (both select hosts in the same manner):

2 Enter the host names that you wish to alter.

*Optionally, you can use the Save or Load buttons to save the entered host names to a file or load a previously saved set of names from a file, respectively. The file structure used is the same as a network scan so that you can also use the saved host names within the main VNC Deployment Tool window.*



3 Optionally click the *Options...* button (available only when performing an install) to check or change the [installation option details](#).

4 Click the *OK* button to proceed with the installation/reinstallation or uninstallation, as selected.

5 A message will be displayed upon completion of the chosen task. If problems were encountered with any hosts, then additional messages will also be displayed.

# Controlling licences

Most VNC products require a valid license key to operate and such licenses are available from RealVNC for varying numbers of hosts. The VNC Deployment Tool allows these licenses to be centrally applied and managed.

A current [scan](#) of the relevant domain or network is required before licenses can be audited.

## Auditing licences

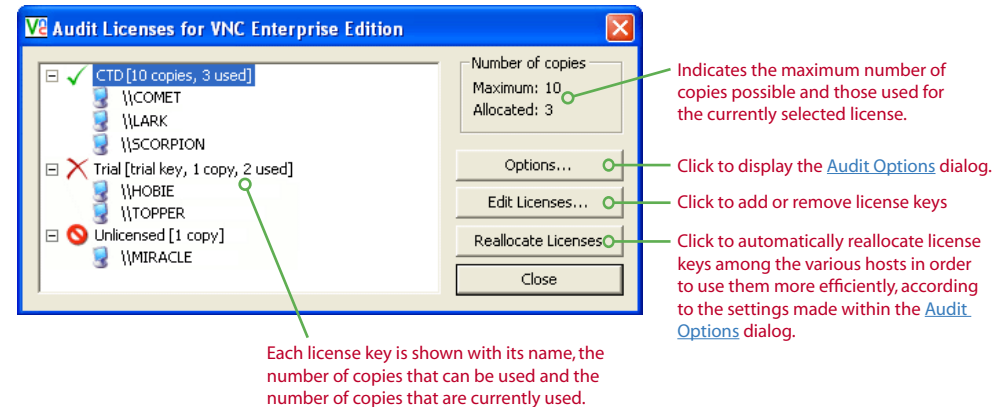
The *Audit Licenses* dialog provides access to all options related to VNC licenses. From this window you can:

- List all current licenses and their allocations ⇨
- [Upgrade out-of-date licenses](#)
- [Manually apply license keys to hosts](#)
- [Automatically reallocate license keys to hosts](#)
- [Change reallocation options](#)
- [Add or remove licenses from VNC Deployment Tool control](#)

### To display the Audit Licenses dialog

- 1 Click the *Licenses* menu and select *Audit Licenses...* (keyboard shortcut: CTRL+A).

The Audit Licenses dialog will be displayed:




The Audit Licenses dialog lists all currently available and used license keys, as well as the hosts that are using them. Shown lower down in the list are hosts that do not possess a license key or hosts that are overusing a key. The following icons are used to indicate various conditions:

### Key to icons

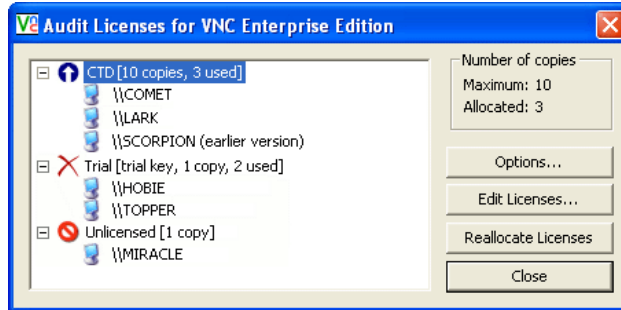
- ✓ The number of hosts using this license key lies within the limit for which it is valid.
- ✗ This license key is *overused*—the number of hosts using it exceeds that for which is valid.
- ⬆ One or more hosts are using an out-of-date version of this license key.
- ⊘ Host(s) using a version of VNC that needs a license key but does not have one installed.
- ? Host(s) using a license key that is valid but is not held within the VNC Tool.
- 💻 Host node.

## Upgrading out-of-date licenses


When a host is discovered with an out-of-date version of a key (which is registered within the VNC Deployment Tool) it will be listed under that key name.

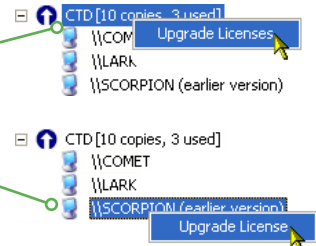
However, the host name will then be marked with the text (*earlier version*) and the icon for that key will change to .

Any hosts using out-of-date license keys may be unable to use the latest versions of VNC until their keys are upgraded.



### To upgrade out-of-date licenses

- 1 Display the [Audit Licenses dialog](#).
- 2 Right click on either:
  - the license key that has the  icon,
  - or
  - the host name that shows (*earlier version*).
- 3 Left click the *Upgrade License* (or *Upgrade Licenses*) option. The later version of the key (if a copy is available) will be applied.



## Reallocating licenses

The VNC Deployment Tool allows you to easily move license keys between hosts in order to make the most efficient use of resources. You can either perform this task manually or allow the VNC Tool do it automatically.

Normally, changing a host's license key takes very little time. However, if the selected host does not currently have a license key, then the `vncconfig` program must be run on it to install one, which can take a few seconds. In this case, a dialog is displayed to inform you of the progress.

### To manually reallocate licenses

- 1 Display the [Audit Licenses dialog](#).
- 2 Click and hold a host name that needs a new license key.
- 3 Drag the host name and drop it onto a license key that has copies available.

If you hold down the *Control* key while dragging, then the `vncconfig` program will be run on the selected host even if it already has a license key. This can be useful in cases where a license key has become corrupted.

### To automatically reallocate licenses

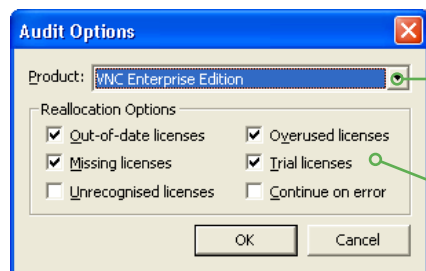
- 1 Display the [Audit Licenses dialog](#).
- 2 Click the *Reallocate Licenses* button.

Depending upon which options are ticked within the audit options dialog, the reallocation will take place *in the following order*, subject to the availability of license keys:

- 1 Upgrade any hosts with out-of-date licenses,
  - 2 Reissue any hosts that are overusing a particular license key (*i.e.* exceeding the number of permitted copies),
  - 3 Allocate a license key to any host operating without one,
  - 4 Allocate a license key to any host using a trial license key,
  - 5 Allocate a license key to any host using an unrecognised key.
- 3 The Audit License view window will reflect the changes made.

## To set audit options

- 1 Display the [Audit Licences dialog](#).
- 2 Click the *Options...* button to display the *Audit Options* dialog:



Indicates the current VNC product for which licenses are to be organised and allows other products to be selected, when available. Each type of VNC product must be audited separately and needs to be selected here.

Reallocation options: These items allow you to determine under which conditions license keys will be reallocated. Hosts that match one or more of the selected conditions will be issued with a new license key from the list held within the VNC Deployment Tool (subject to availability). Reallocation options are prioritised in the following order: Out-of-date licenses > Overused licenses > Missing licenses > Trial licenses; > Unrecognised licenses See [Reallocating licenses](#) for details.

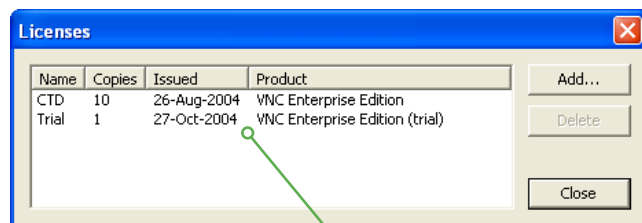
- 3 Make the necessary changes to the options and click *OK*.

## To add or remove license keys

This task is carried out using the *Licenses* dialog which can be accessed in two ways:

- From the main VNC Deployment Tool window: Click the *Licenses* menu and select *Add/Remove Licenses...* (keyboard shortcut: CTRL+L).
- From the *Audit Licenses* dialog: Display the [Audit Licenses dialog](#) and click the *Edit Licenses...* button.

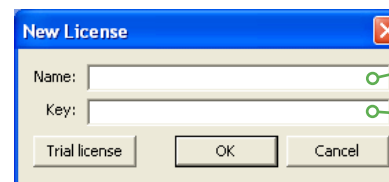
The Licenses dialog will be displayed:



Lists all currently held license keys including the number of copies that can be used, the date they were issued and the VNC product that they cover.

## To add a new license key

- 1 Display the *Licenses* dialog (see opposite).
- 2 Click the *Add...* button to display the *New License* dialog:



Enter a name for the new license that is not used by any currently held license key.

Enter the license key number e.g. A1B23-CD4EF-5GH6I-7JK89-L0MNO

- 3 Enter any mnemonic name for the new license that is not already being used by another license.
- 4 Enter the license key as supplied by RealVNC. Valid license keys have five blocks of five alphanumeric characters, separated by dashes.

*Trial License:* If you are evaluating this product for the first time, the *Trial license* button will be available. If you click this, a license key will be granted for up to ten hosts within a limited period of thirty days. This offer is available once, after which a full license will need to be purchased.

- 5 Click the *OK* button. The new license key will be added to the list and can now be applied to one or more hosts. See [Reallocating licenses](#) for more details.

## To delete a license key

- 1 Display the *Licenses* dialog (see opposite).
- 2 Click on the name of the license to be removed.
- 3 Click the *Delete* button.
- 4 Click the *Yes* button to confirm the action.

# Configuring settings

The VNC Deployment Tool allows you to remotely control the individual settings of VNC installations. Hosts can be:

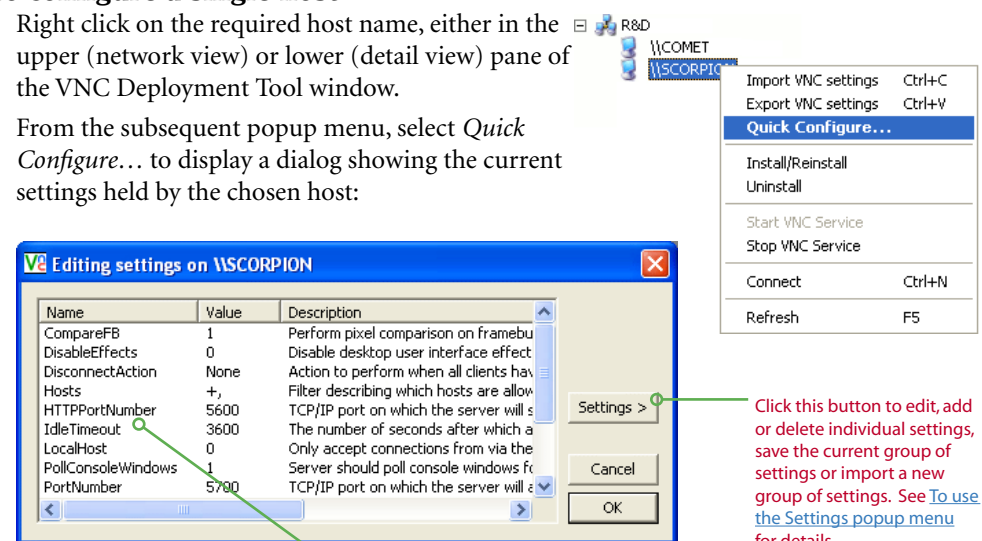
- Configured individually (see opposite), or
- A set of common settings can be applied to [multiple hosts](#) under your administration.

*Note: Settings held by hosts will remain unaffected by a configuration session unless they are specifically altered by the VNC Deployment Tool.*

## Configuring a single host

### To configure a single host

- 1 Right click on the required host name, either in the upper (network view) or lower (detail view) pane of the VNC Deployment Tool window.
- 2 From the subsequent popup menu, select *Quick Configure...* to display a dialog showing the current settings held by the chosen host:



Settings are listed by in alphabetical order by name, with their current values and a description.

- 3 Use the [Settings popup menu](#) to add, edit, delete, import, save or load items as required.
- 4 When all changes are complete, click the OK button.  
Any changes to the settings will be automatically exported to the selected host.

# Configuring multiple hosts

When configuring more than one host, you can alter the precise method used depending on how many settings will be changed:

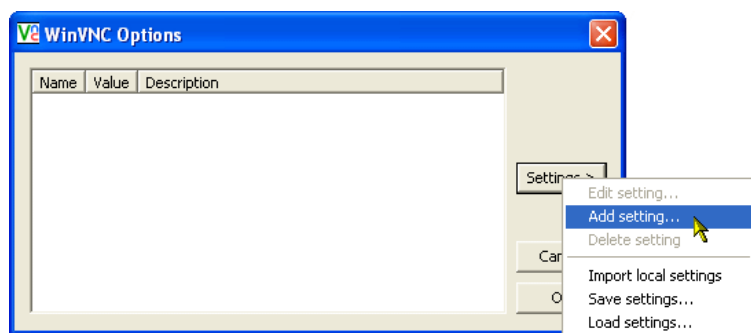
- To adjust only a small number of specific host settings: it can be quicker to create a new small list of settings by selecting only the required ones from the *Add setting...* option.
- To globally change all (or nearly all) host settings: it is quicker to import settings from a sample host (either the local system or one of the remote hosts), modify the parameters where necessary and send them.

*Remember: Settings held by hosts will remain unaffected by a configuration session unless they are specifically altered by the VNC Deployment Tool.*

## To configure multiple hosts

*Note: If you wish to import a list of sample settings from a remote host, right click on the host name within the upper or lower pane of the VNC Development Window and select 'Import VNC Settings' from the popup menu.*

- 1 Click the *Configuration* menu and select *Edit Configuration...* (keyboard shortcut: SHIFT+F2). The *WinVNC Options* dialog will be displayed; if sample settings were imported, then these will be shown:

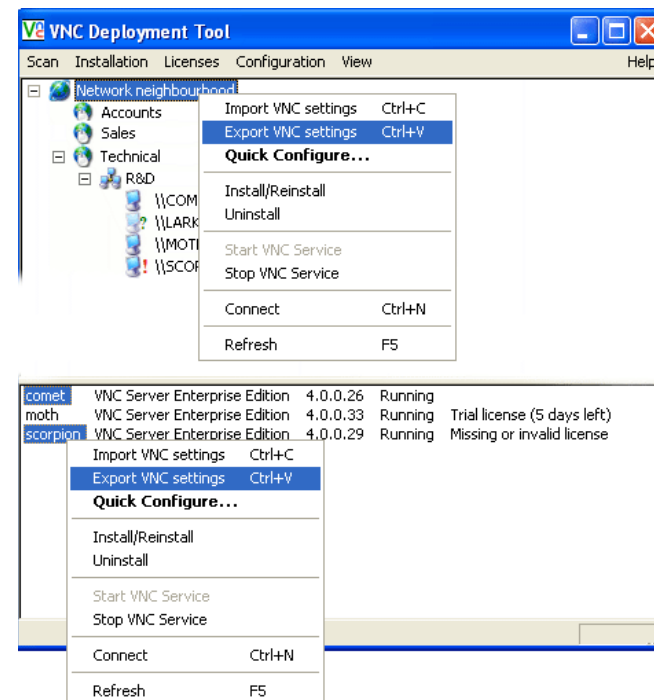


- 2 Either, right-click in the setting window or click the *Settings >* button to display the settings popup. Use the [Settings popup menu](#) to add, edit, delete, import, save or load items, as required. Most notably, the *Import local settings* option lets you use the local system settings as the template for the remote hosts.
- 3 When all changes are complete, click the *OK* button.

- 4 Choose the hosts to be altered:

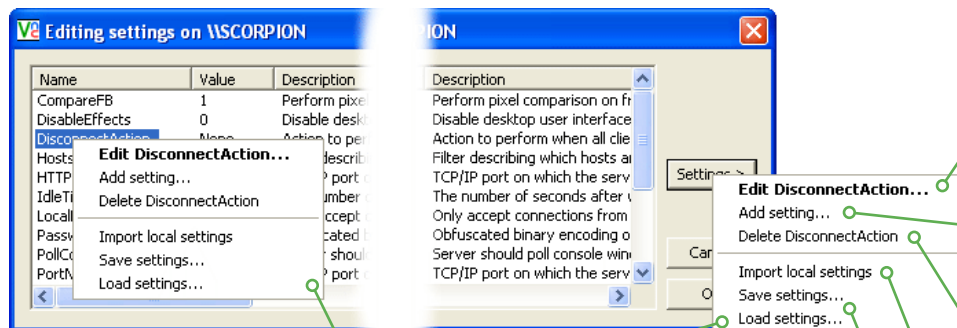
- Use CTRL and click to select individual host names in the lower (Detail view) pane,
- Use SHIFT and click to select a range of hosts in the lower (Detail view) pane, or
- Select a domain or network name in the upper (Network view) pane (this will affect all descendants of the selected node).

- 5 Right click on one of the selected hosts and select *Export VNC Settings* (keyboard shortcut: CTRL+V) to send.
- 6 The settings will be exported to the selected host and a message will be displayed upon completion.



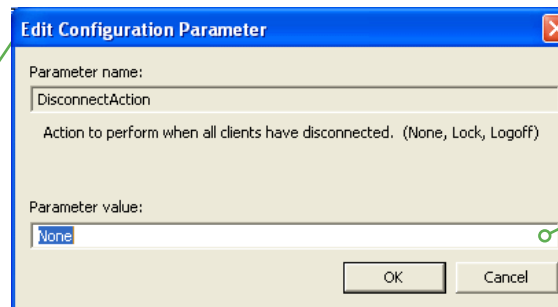
## To use the Settings popup menu (to add or edit a setting)

- 1 Display either the *Quick configure* dialog (right click on a host name and select *Quick Configure...*) or the *WinVNC Options* dialog (click the *Configuration* menu and select *Edit Configuration...*).
- 2 In the dialog, either right-click on a setting name or click the *Settings >* button to display the settings popup:

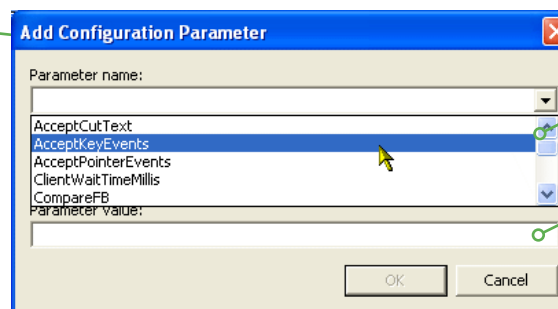


The Settings popup menu can be accessed with a right click on a setting name or by clicking the Settings button.

- 3 Select the required option from the popup menu:



Alter the *Parameter value*, as necessary, within the permitted range. See [Settings index](#) for more details about settings and their ranges.



Select the appropriate setting from the *Parameter name* drop down list.

Alter the *Parameter value*, as necessary, within the permitted range. See [Settings index](#) for more details about settings and their ranges.

Removes the currently selected setting from the list. The precise effect of this action will depend on whether you selected this dialog from the Quick Configure option or via the Edit Configuration option.

- *via Quick configure*: The setting that you delete will be similarly removed from the host system's registry, with the effect that the setting will revert to its default value.
- *via Edit configuration*: The setting that you delete will merely be omitted from the list. When the settings are later exported, that particular item will not be sent and so will not affect the similar setting (if present) on the host(s).

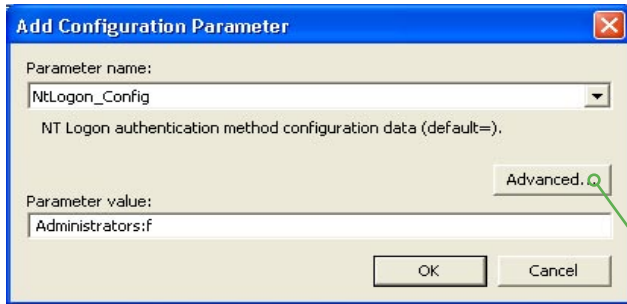
Overwrites the current settings list with one from the VNC installation on the local system. This can then be used to change the remote system.

Allow you to save and load settings as .reg files. These can be reused within VNC Deployment Tool, or using Regedit or Windows Explorer.

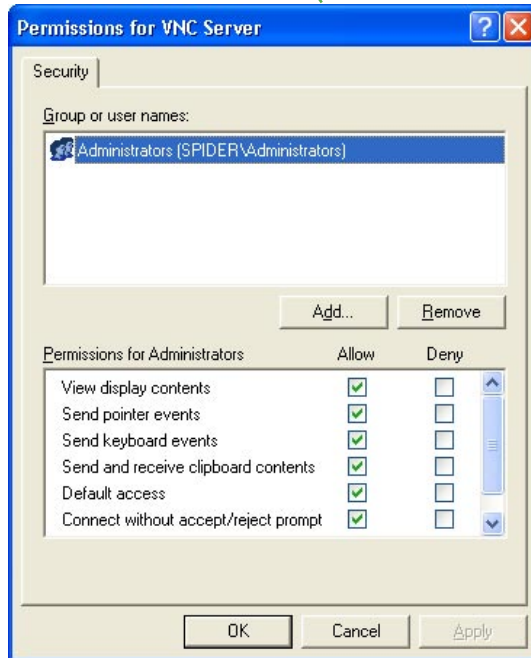
# Configuring NtLogon Access Control

The NtLogon access control is stored in a parameter named `NtLogon_Config`. You can add or modify this parameter by following the steps described in [Configuring Settings](#). The access control can be specified in two ways:

- Using the syntax described in the [NtLogon Config](#) section.
- Using the standard Windows access control dialog (on platforms that support it).



To use the standard Windows access control dialog, click on the **Advanced...** button. The current access control will be displayed in the access control dialog and can be edited as described in the VNC Server for Windows user guide. If no access control is currently configured, then the dialog displays the default VNC access control.



# Configuring Password Parameters

The VNC server has four password parameters that are used if it is configured to use VNC password authentication. These options are `AdminPassword`, `InputOnlyPassword`, `Password` and `ViewOnlyPassword`, corresponding to the users `Admin`, `InputOnly`, `User` and `ViewOnly`, respectively. For security reasons, these cannot be entered using the same interface as other configuration parameters, as this would display the password in plaintext on the screen. Instead, these four options are all configured or disabled by clicking on the **Advanced...** button.



Use this dialog to enable or disable the account. If enabling an account, then you will need to enter and confirm the new password for that account, otherwise no password will be required to access the account. Note that if you dismiss the first dialog without clicking on the **Advanced...** button, then the **Configure Login** dialog will be shown automatically to prevent accidentally creating an account with no password.



# Settings index

This section provides you with explanations of all settings that can be applied to remote VNC hosts using the VNC Deployment Tool. The settings are given here alphabetically as they appear within the settings list. They are also given, on the pages that follow, against the settings within the tabs of the VNC Server options window that they emulate.

## Main tab settings

Setting name	VNC Server tab	Value/Range
<a href="#">AcceptCutText</a>	Inputs	0 (disable), 1 (enable)
<a href="#">AcceptKeyEvents</a>	Inputs	0 (disable), 1 (enable)
<a href="#">AcceptPointerEvents</a>	Inputs	0 (disable), 1 (enable)
<a href="#">AdminPassword</a>	Security	Password
<a href="#">AlwaysShared</a>	Sharing	0 (disable), 1 (enable)
<a href="#">CompareFB</a>	Capture Method (Hooks)	0 (disable), 1 (enable)
<a href="#">DisableEffects</a>	Desktop	0 (disable), 1 (enable)
<a href="#">DisableLocalInputs</a>	Inputs	0 (disable), 1 (enable)
<a href="#">DisconnectAction</a>	Desktop	None, Lock, Logoff
<a href="#">DisconnectClients</a>	Sharing	0 (disable), 1 (enable)
<a href="#">GuestAccess</a>	Security	Access rights
<a href="#">Hosts</a>	Connections	IP address list & range masks
<a href="#">HTTPPortNumber</a>	Connections	0 to 65535
<a href="#">IdleTimeout</a>	Connections	0 (disable) to any value
<a href="#">InputOnlyPassword</a>	Security	Password
<a href="#">LocalHost</a>	Connections	0 (disable), 1 (enable)
<a href="#">NeverShared</a>	Sharing	0 (disable), 1 (enable)
<a href="#">NTLogon_Config</a>	(Security)	Access control
<a href="#">Password</a>	Security	Password
<a href="#">PollConsoleWindows</a>	Capture Method (Hooks)	0 (disable), 1 (enable)
<a href="#">PortNumber</a>	Connections	0 to 65535
<a href="#">Protocol3.3</a>	Legacy	0 (disable), 1 (enable)
<a href="#">QueryConnect</a>	Security	0 (disable), 1 (enable)
<a href="#">QueryOnlyIfLoggedOn</a>	Security	0 (disable), 1 (enable)
<a href="#">RemovePattern</a>	Desktop	0 (disable), 1 (enable)
<a href="#">RemoveWallpaper</a>	Desktop	0 (disable), 1 (enable)
<a href="#">ReverseSecurityTypes</a>	(Security)	None, RA2
<a href="#">SecurityTypes</a>	Security	None, VncAuth, RA2, RA2ne
<a href="#">SendCutText</a>	Inputs	0 (disable), 1 (enable)

<a href="#">UpdateMethod*</a>	Capture Method (Hooks)	0 (disable), 1 (enable)
<a href="#">UseCaptureBlt</a>	Capture Method (Hooks)	0 (disable), 1 (enable)
<a href="#">UseHooks*</a>	Capture Method (Hooks)	0 (disable), 1 (enable)
<a href="#">UserPasswdVerifier</a>	Security	None, VncAuth, NtLogon
<a href="#">ViewOnlyPassword</a>	Security	Password

\* The setting 'UseHooks' is replaced by 'UpdateMethod' from Enterprise version 4.1 onward.

## Extra settings

Setting name	VNC Server tab	Value/Range
<a href="#">AutoKeyboardLayout</a>	none (extra setting)	0 (disable), 1 (enable)
<a href="#">BlacklistThreshold</a>	none (extra setting)	Number of attempts
<a href="#">BlackListTimeout</a>	none (extra setting)	Time period in seconds
<a href="#">ClientWaitTimeMillis</a>	none (extra setting)	Time period in milliseconds
<a href="#">DeadKeyAware</a>	none (extra setting)	0 (disable), 1 (enable)
<a href="#">DisableAddNewClient</a>	none (extra setting)	0 (allow), 1 (disable)
<a href="#">DisableClose</a>	none (extra setting)	0 (allow), 1 (disable)
<a href="#">DisableOptions</a>	none (extra setting)	0 (allow), 1 (disable)
<a href="#">DisplayDevice</a>	none (extra setting)	Device name
<a href="#">EnableGuestLogin</a>	none (extra setting)	0 (disable), 1 (enable)
<a href="#">GuestPassword</a>	none (extra setting)	Password
<a href="#">GuestUserName</a>	none (extra setting)	User name
<a href="#">Log</a>	none (extra setting)	Log file details
<a href="#">MaxCutText</a>	none (extra setting)	Clipboard size in bytes
<a href="#">QueryTimeout</a>	none (extra setting)	Time period in seconds
<a href="#">QueryTimeoutRights</a>	none (extra setting)	Access control
<a href="#">RemapKeys</a>	none (extra setting)	Hexadecimal mapping list
<a href="#">ZlibLevel</a>	none (extra setting)	Compression level

## Settings from the Security tab

### UserPasswdVerifier

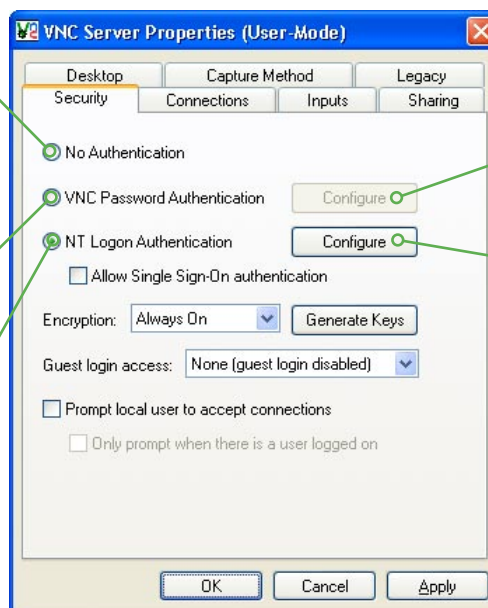
Configures the authentication method to be used for viewers connecting to each server.

[None] When selected, this option will allow the viewer application to connect with the VNC Server without the need for username or password. This option can be useful when the server system is operating within a secure environment, or may be used when tunnelling VNC over a secure protocol, such as SSH (Secure Shell), to remove a redundant level of authentication.

**IMPORTANT:** Use this option with extreme caution. Do NOT use it unless the host network is known to be completely secure.

[VncAuth] When selected, this option will require the viewer application to supply a valid password (as defined by the *Password*, *AdminPassword*, *ViewOnlyPassword* or *InputOnlyPassword* settings) before granting access to the server system.

[NtLogon] This option (not available on Windows 95, 98 or Me installations) links into the internal security system within Windows NT, 2000, 2003 Server and XP. The advantage of this method is that, using the Windows user configurations, you can create different permissions for different types of users, e.g. administrators, guests, users, etc. Use the [NTLogon Config](#) option to configure access control.



### Password, AdminPassword, InputOnlyPassword and ViewOnlyPassword

Configures the passwords that will be used when the *UserPasswdVerifier* setting is configured as *VncAuth*.

### NTLogon\_Config

This parameter is entered as a comma-separated list of credentials, where each credential consists of an account name, followed by a colon and the required access rights. The access rights are as follows:

- v* View display contents
- p* Send pointer events
- k* Send keyboard events
- c* Send and receive clipboard contents
- d* Default access. Currently equivalent to options: *v p k* and *c*.
- q* Connect without accept/reject prompt
- f* Full access. Currently equivalent to options: *v p k c* and *q*.

Consider the example:

*HOME\administrator:f;VNC Users:d*

This grants the *administrator* account on the HOME domain full access and also grants the local group *VNC Users* default access.

In general, each account name is either a fully qualified domain account name of the form DOMAIN\acct or an unqualified local account name. Local accounts can also be specified as fully qualified names of the form HOST\acct, but this is not necessary.

## GuestAccess

The *GuestAccess* parameter determined the level of access for the *guest* login, when enabled. It is expressed as a string in the same format as is used for the [NtLogon Config](#) parameter. The values that can be set using the *vnconfig* applet are as follows:

None (guest login disabled)	0 or empty
View-only	v
Interactive	d

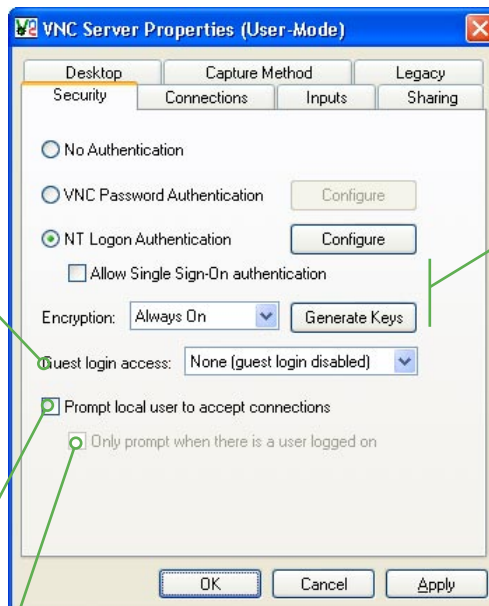
However, any valid permissions string can be set here.

## QueryConnect

If *QueryConnect* is set to '1', the local user of the server system must accept all connections before the incoming viewer application is granted access. If no response is given within ten seconds, the connection is rejected. This timeout can be configured using the [QueryConnectTimeout](#) parameter, but has no corresponding user interface element. If a second viewer attempts to connect during this time, then it will be immediately rejected.

## QueryOnlyIfLoggedOn

If *QueryOnlyIfLoggedOn* is set to '1', connections incoming when there is no-one logged on are treated as if *QueryConnect* was set to '0'.



## SecurityTypes and ReverseSecurityTypes

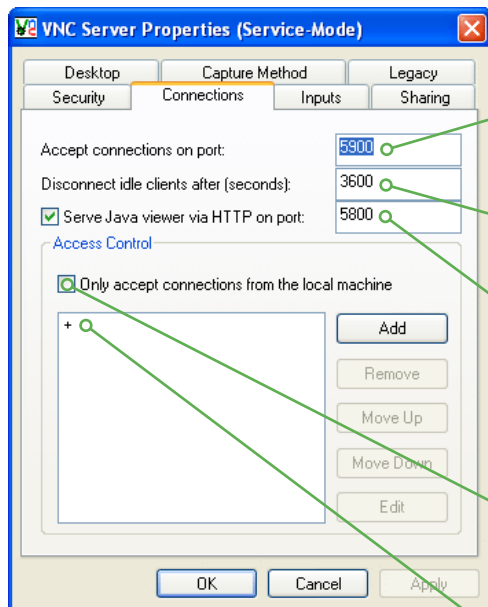
Determines how encryption will be applied to incoming (*SecurityTypes*) and outgoing (*ReverseSecurityTypes*) user connections. The recognised values are as follows:

- RA2[ne] Encrypted session [password only]
  - VncAuth Challenge-response password
  - None Unencrypted password and session
  - SSPI[ne]\* Single sign-on, encrypted session [password only]
- \*Note that single sign-on is only available from VNC Enterprise Edition viewers running on Windows platforms

Use combinations of these values as shown below to emulate the VNC Server settings:

Authentication	Encryption	SecurityTypes	ReverseSecurityTypes
No Authentication	Prefer Off	RA2ne,None,RA2	None,RA2
	Prefer On	RA2,RA2ne,None	RA2,None
	Always On	RA2	RA2
VNC Password Authentication	Prefer Off	RA2ne,VNCAuth,RA2	None,RA2
	Prefer On	RA2,RA2ne,VNCAuth	RA2,None
	Always On	RA2	RA2
NT Logon Authentication with Single Sign-On	Prefer Off	SSPIne,RA2ne,SSPI,RA2	None,RA2
	Prefer On	SSPI,RA2,SSPIne,RA2ne	RA2,None
	Always On	SSPI,RA2	RA2
NT Logon Authentication without Single Sign-On	Prefer Off	RA2ne,RA2	None,RA2
	Prefer On	RA2,RA2ne	RA2,None
	Always On	RA2	RA2

## Settings from the Connections tab



### PortNumber

Sets the port through which viewer clients will be served. The standard setting of 5900 is expected by VNC Viewer applications; however, if this port clashes with another local network service, then it can be changed to use any other vacant port number. Please note, however, if you alter this number, then the viewer user(s) will need to specify the non-standard port number as part of the network address when logging-in.

### IdleTimeout

Determines the maximum period of time (in seconds) that a viewer can remain logged-in, yet inactive. After the set period of time has elapsed since the last user interaction, VNC Server will terminate the connection in order to conserve resources. As standard this option is set to 3600 seconds, or 1 hour. To prevent any connection timeouts, set this option to 0 (zero).

### HTTPPortNumber

Determines the port through which VNC Server will provide the Java viewer applet to capable web browsers, when requested. This value is normally 100 less than the Hosts port, although they can be set to the same port. Set this option to zero to disable the feature.

### LocalHost

When set to '1', this option will cause the access control settings (if any) to be ignored and make the VNC Server system to be inaccessible via all network interfaces except the local loopback interface. This option is normally used only when tunnelling VNC sessions into the server, for instance via the SSH (Secure Shell) protocol.

### Hosts

Defines specific addresses or ranges of addresses that are to be included (denoted by a '+' prefix), excluded (denoted by a '-' prefix) or queried (denoted by a '?' prefix). *Note: Query means that the local user of a server system must approve the connection within ten seconds.*

Each entry in the list is expressed as an IP address plus a 'subnet-style' range mask separated by a slash '/'. Multiple hosts entries are separated by a comma. Consider the example entry below:

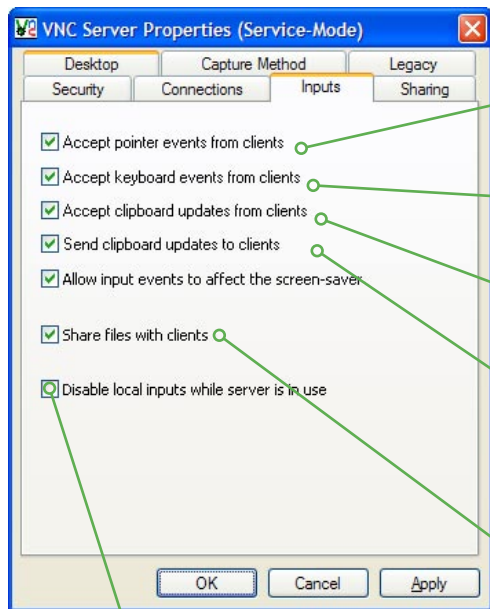
`+192.168.0.1/255.255.255.255,?192.168.4.0/255.255.255.0,-0.0.0.0/0.0.0.0`

- The first entry includes access from a single specific address of 192.168.0.1
- The second entry queries any access from any machine situated in the 192.168.4 subnet.
- The third entry denies access from any other IP address.

To exclude particular addresses (or small ranges) from within an included range, add the address and suitable subnet mask **after** the include entry and prefixed with '-'.

For more details about including, excluding and querying addresses, please see the VNC Server 4 user guide.

## Settings from the Inputs tab



### AcceptPointerEvents

When set to '1', the viewer user is permitted to control the server using their mouse. In combination with the *AcceptKeyEvents* and *AcceptCutText* options, disabling (set to '0') this control is useful for making the server a 'view only' system.

### AcceptKeyEvents

When set to '1', the viewer user is permitted to control the server using their keyboard. In combination with the *AcceptPointerEvents* and *AcceptCutText* options, disabling (set to '0') this control is useful for making the server a 'view only' system.

### AcceptCutText

When set to '1', the viewer user can copy items from their system to the clipboard of the server. In combination with the *AcceptPointerEvents* and *AcceptKeyEvents* options, disabling (set to '0') this control is useful for making the server a 'view only' system.

### SendCutText

When set to '1', any data added to the clipboard of the server system will be made available to the clipboard of any viewer user who is logged-in at the time. Disabling this option (set to '0') can be useful in preventing private server information from being leaked via the clipboard by untrusted viewer users.

### ShareFiles

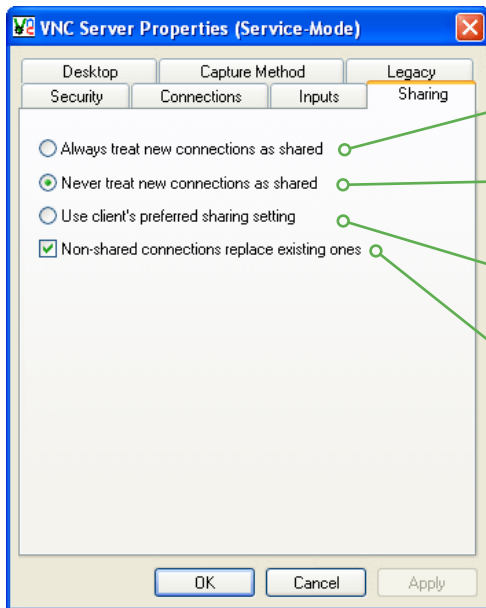
When set to '1', this option enables file transfer between the server and capable viewers.

### DisableLocalInputs

When set to '1', this option ignores any input from the server's own locally connected keyboard and/or mouse while the viewer user is connected.

**Note:** The remaining option on this page, *Allow input events to affect the screen-saver*, is a system-wide setting and cannot be configured remotely using the VNC Deployment Tool.

## Settings from the Sharing tab



### **AlwaysShared = 1, NeverShared = 0**

All incoming connections will be treated as shared and so no existing users will be disconnected nor will new users be turned away.

### **AlwaysShared = 0, NeverShared = 1**

All incoming connections will be treated as non-shared. When a second incoming connection attempt is made, it will either be rejected or the existing user will be disconnected, depending upon the setting of the *DisconnectClients* option.

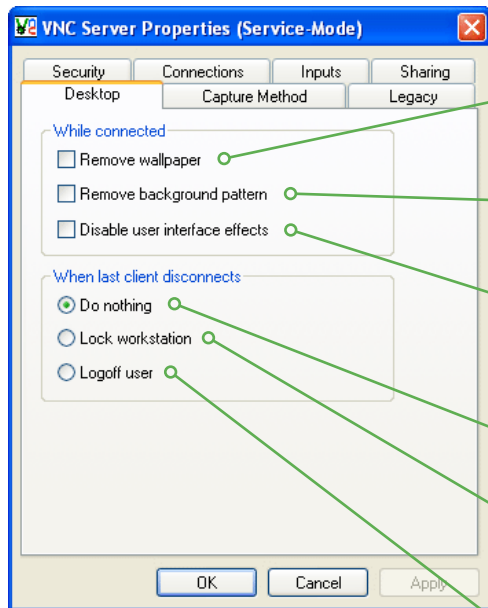
### **AlwaysShared = 0, NeverShared = 0**

VNC Server will defer to the 'Shared connection' setting of the second incoming viewer. If the second viewer is set to share, then it will be permitted to make the connection, if not it will either be rejected or will replace the existing viewer, depending upon the setting of the *DisconnectClients* option.

### **DisconnectClients**

Determines the outcome when a connection is non-shared, either by viewer choice or when the *AlwaysShared* = 0 and *NeverShared* = 1. In such cases, if this option is set to '1', then the existing user is disconnected. If this option is set to '0', then the new user is rejected.

## Settings from the Desktop tab



### **RemoveWallpaper**

When set to '1', the wallpaper image (if used) on the server system will be removed and replaced with a plain background whenever a VNC viewer is connected. This can help to reduce transmitted data and hence improve overall performance.

### **RemovePattern**

When set to '1', the background pattern (if used) on the server system will be removed and replaced with a plain background whenever a VNC viewer is connected. This can help to reduce transmitted data and hence improve overall performance.

### **DisableEffects**

When set to '1', any visual user interface effects, such as animated drop-down boxes, will be disabled whenever a VNC viewer is connected. This can help to reduce transmitted data and hence improve overall performance.

### **DisconnectAction = None**

When set to 'None', there will be no change to the operation of the server once there are no more VNC viewers connected to it.

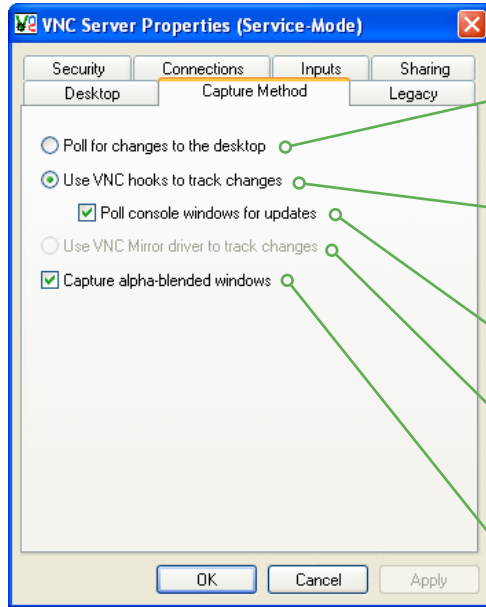
### **DisconnectAction = Lock**

When set to 'Lock', after the last VNC viewer has disconnected, the server system will be temporarily locked and returned to its log-in screen. This option can help to avoid un-authorized access where the system is left unattended and other people are in its vicinity.

### **DisconnectAction = Logoff**

When set to 'Logoff', after the last VNC viewer has disconnected, the current user session of the server system will be ended and the system returned to its initial log-in screen. This option is useful to ensure that the server system never remains logged-on after a VNC session. This option can help to avoid un-authorized access where the system is left unattended and other people are in its vicinity.

## Settings from the Capture method (Hooks) tab



*Note: This tab is titled Hooks within VNC versions prior to v4.1.*

### **UpdateMethod=poll \***

When set to 'poll', this option polls the Windows display system for changes to the entire desktop. This method is slower than the 'hooks' and 'mirror' options. However, it can be useful in cases where the other two methods encounter timing/compatibility problems or cannot track an application that interfaces directly with the graphics card, such as with some DirectX applications.

### **UpdateMethod=hooks \***

When set to 'hooks', this option employs the standard VNC hooks technique to monitor changes to the local desktop. VNC hooks allow VNC Server to monitor the messages sent to on-screen windows in order to ascertain when their content may have changed. This method is very successful; however, it can miss certain types of update or conversely can also mistakenly report areas as having changed when in fact they have not. For these reasons, you are recommended to use this method in conjunction with 'PollConsoleWindows' option.

### **PollConsoleWindows**

When set to '1', this option will track the visible parts of console windows and poll those areas for changes. This option is best used in close combination with the 'UseHooks' option because the rate of polling can be reduced, which helps to increase performance.

### **UpdateMethod=mirror**

When set to 'mirror', this option takes advantage of a Windows facility that mirrors all primary display graphical updates to a secondary driver, such as VNC. This produces a fast and accurate update method, however, it operates at a low system level and could encounter problems on some systems.

### **UseCaptureBlt**

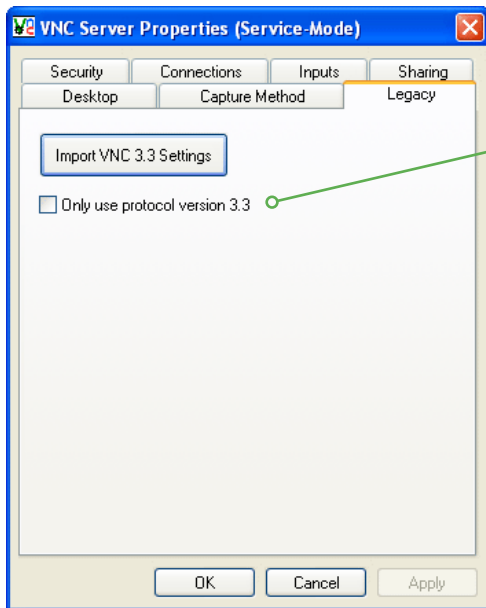
When set to '1', this option tracks standard windows as well as the newer semi-transparent windows, including certain menus and tool tips. This method places higher requirements on the server and can induce cursor flicker.

### **\* In versions prior to 4.1**

UseHooks=1 selects the VNC Hooks method.

UseHooks=0 selects the Poll for changes to the desktop method.

## Settings from the Legacy tab



### Protocol3.3

When set to '1', the VNC Server will restrict its operation to use only the version 3.3 protocol. This option is most useful when being accessed by third-party VNC applications that report non-standard version numbers and hence, may cause incompatibility issues.

*Warning: Use this option with caution as security settings can be weakened in order to support older viewers.*

## Extra settings

This section provides extra settings that are not available on the tabbed pages of VNC Server but can be configured on remote hosts by the VNC Deployment Tool.

### AutoKeyboardLayout

When set to '1', the server's keyboard layout will temporarily be switched if a symbol is received that cannot be generated with the current keyboard layout.

### BlacklistThreshold

Sets the number of unauthenticated connection attempts allowed from any individual host before that host is black-listed. See also *BlackListTimeout*.

### BlackListTimeout

Sets the initial timeout applied when a host is first black-listed. The host cannot re-attempt a connection until the timeout value, in seconds, expires. See also *BlackListThreshold*.

### ClientWaitTimeMillis

Sets the time period, in milliseconds, to wait for a client that is no longer responding.

### DeadKeyAware

When set to '1', assumes the viewer has already interpreted dead key sequences into latin-1 characters.

### DisableAddNewClient

When set to '1', disables the *Add New Client* entry in the VNC Server tray menu.

### DisableClose

When set to '1', disables the *Close* entry in the VNC Server tray menu.

### DisableOptions

When set to '1', disables the *Options* entry in the VNC Server tray menu.

### DisplayDevice

Display the device name of the monitor to be remoted, for example '\\.\DISPLAY1', or empty to export the whole desktop.

### EnableGuestLogin

When set to '1', the *guest* login will initially be enabled when VNC server starts up.

### GuestPassword

Obfuscated binary encoding of the password that must be entered to login as the guest user, or empty if no password is required.

### GuestUserName

The username that must be entered to log in as a guest when this feature is enabled, or empty to use the default of *guest*.

### Log

Specifies which log output should be directed to which target logger, and the level of output to log. Format is <log>:<target>:<level>[, ...].

### QueryTimeout

Sets the time period, in seconds, that the local user of the server system is given to approve a queried incoming connection before it is automatically allowed or denied access.

### QueryTimeoutRights

Sets the access rights that a timed-out connection query grants, in the format used for the [NtLogon\\_Config](#) parameter.

### RemapKeys

Specifies a mapping for incoming keys. It is specified as a comma-separated list of mappings, each of which is a pair of hexadecimal keysyms separated by -> or <>. For example, to exchange the “ and @ symbols, use the mapping 0x22<>0x40.

### ZlibLevel

Sets the compression level for Zlib encoding, from 0 to 9 or -1 to select the default .

## Support

If you are unable to solve your problem after checking through the Troubleshooting section in this guide, please take a look at our on-line [FAQ page](#) and also the [Known Bugs & Features](#) section of the RealVNC website.

If you still cannot find a solution, then please contact us for further assistance:

### Via the web

The [www.realvnc.com](http://www.realvnc.com) website offers a number ways to gain assistance regarding VNC products:

#### Search indexes

Provides an opportunity to search through the various VNC databases for solutions

[www.realvnc.com/swish-e/search](http://www.realvnc.com/swish-e/search)

#### Mailing lists

Real VNC provide discussion forums for important announcements and many other VNC-related subjects. You can browse or search previous discussion entries, or alternatively subscribe to one or more forums.

[www.realvnc.com/lists.html](http://www.realvnc.com/lists.html)

#### Product support request

This section lets you to send queries directly to the VNC development team.

[www.realvnc.com/cgi-bin/support.cgi](http://www.realvnc.com/cgi-bin/support.cgi)

### By post

RealVNC Limited  
17d Sturton Street  
Cambridge  
CB1 2SN

Documentation by:  [www.ctxd.com](http://www.ctxd.com)

# Index

## A

- AcceptCutText 19
- AcceptKeyEvents 19
- AcceptPointerEvents 19
- Accept clipboard updates 19
- Accept keyboard events 19
- AlwaysShared 20
- Audit Licenses 8

## B

- BlacklistThreshold 24
- BlackListTimeout 24

## C

- Capture alpha-blended windows 22
- ClientWaitTimeMillis 24
- CompareFB 22
- Configure
  - multiple hosts 12
  - single host 11
- Credentials 5

## D

- DeadKeyAware 24
- Detail view 3
- DisableEffects 21
- DisableLocalInputs 19
- DisableOptions 24
- DisconnectAction 21
- DisconnectClients 20
- DisplayDevice 24

## E

- Encryption 17

## F

- FAQ 25

## H

- Hosts 18
- HTTPPortNumber 18

## I

- Icons
  - license audit 8
  - network scan 4
- IdleTimeout 18
- Install options 6

## L

- Licenses 8
  - reallocating 9
  - upgrading 9
- License keys
  - add/remove 10
- LocalHost 18
- Log 24

## N

- Network view 3
- NeverShared 20

## O

- Options
  - audit 10
  - install 6

## P

- Password 16
- Password settings 6
- PollConsoleWindows 22
- Poll console windows 22
- Protocol3.3 23

## Q

- QueryConnect 17

## R

- Reallocating licenses 9
- RemovePattern 21
- RemoveWallpaper 21
- Rescan a single node 5

## S

- Scanning
  - options 5
- Scanning options 5
- Scanning the network 4
- Scans
  - saving and loading 5
  - using credentials 5
- SecurityTypes 17
- SendCutText 19
- Send clipboard updates 19
- Settings
  - index 15
  - popup menu 13
- Support 25
  - getting assistance 25

## U

- Upgrading licenses 9
- UseCaptureBlt 22
- UseHooks 22
- UserPasswdVerifier 16

## W

- When last client disconnects 21

## Z

- ZlibLevel 24