RLD Automation

FactoryLink server

Brabant Water
DWP Schijf

UltraVNC

RLD
Automation

v. Sonsbeeckstraat 11
5344 JB Oss

Tel: 0412-655909
Mail: mjordaan@rldautomation.eu

Industriële Automatisering

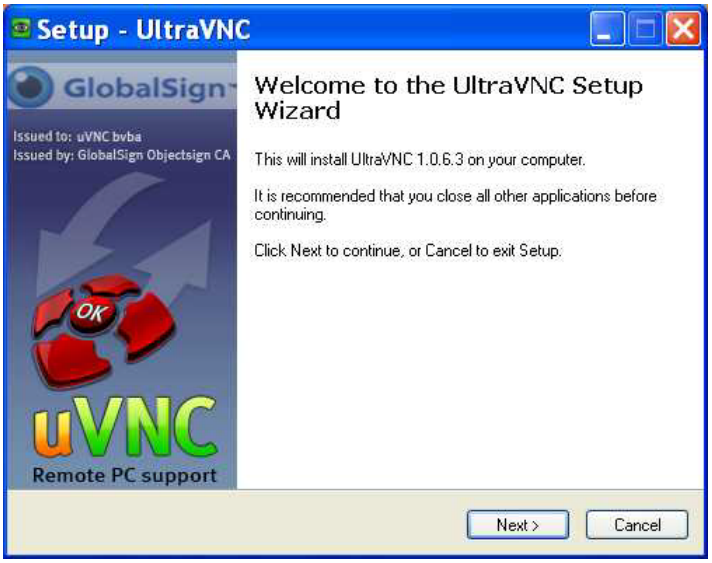
Opdrachtgever: Brabantwater
Project: DWP Schijf
Project id: V109020

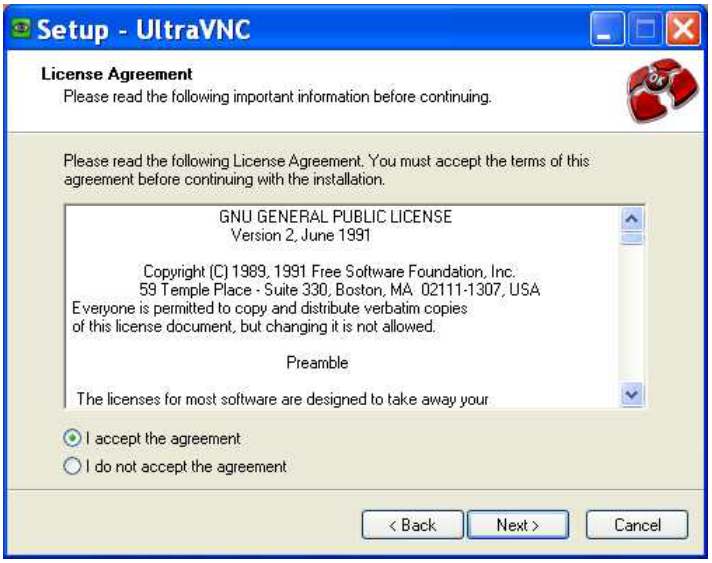
brabant water

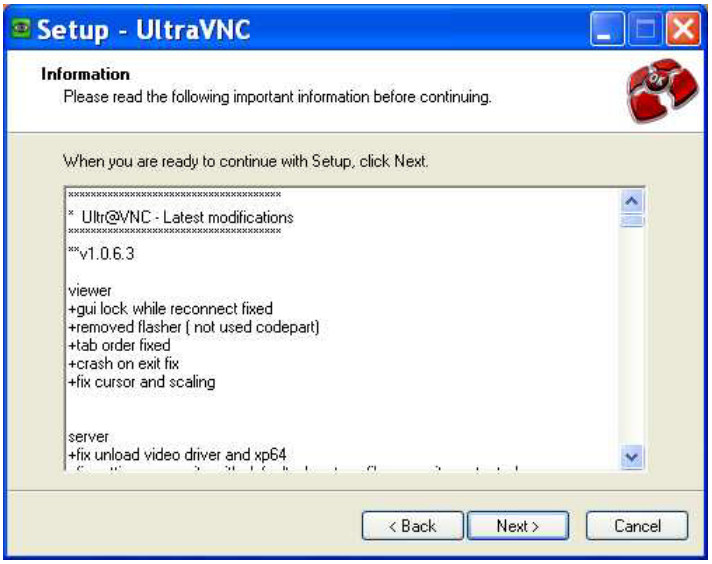
Inhoudsopgave

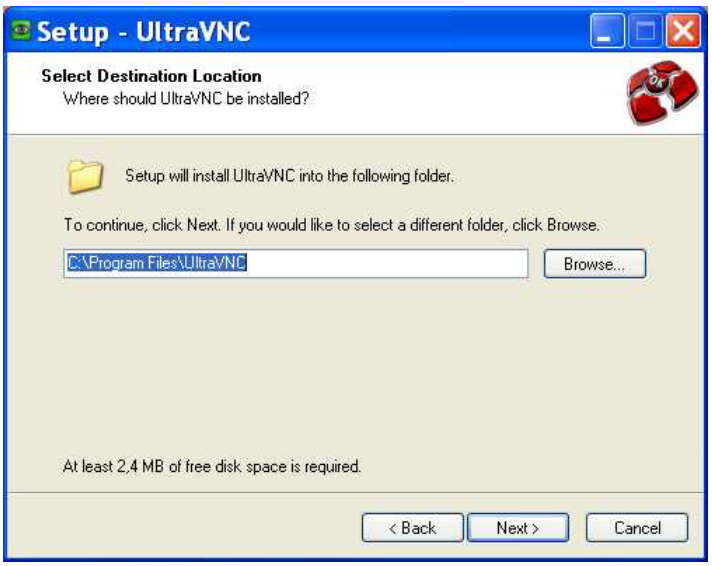
1 Installation

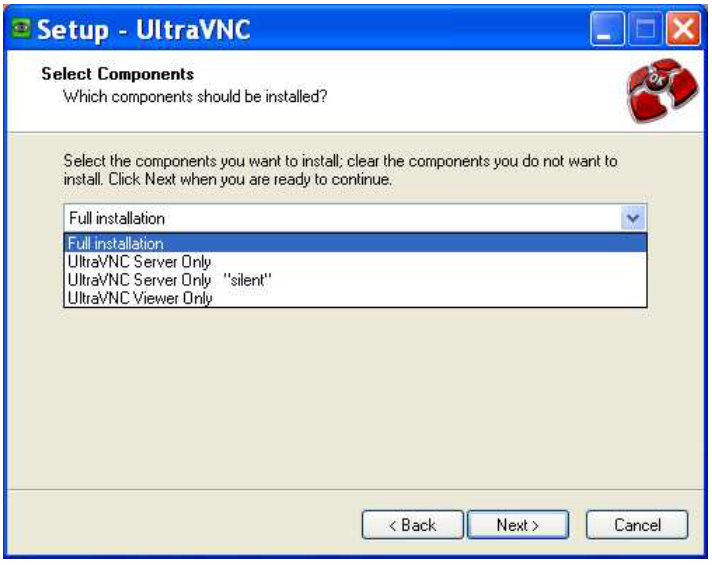
1.1 Installation UltraVNC

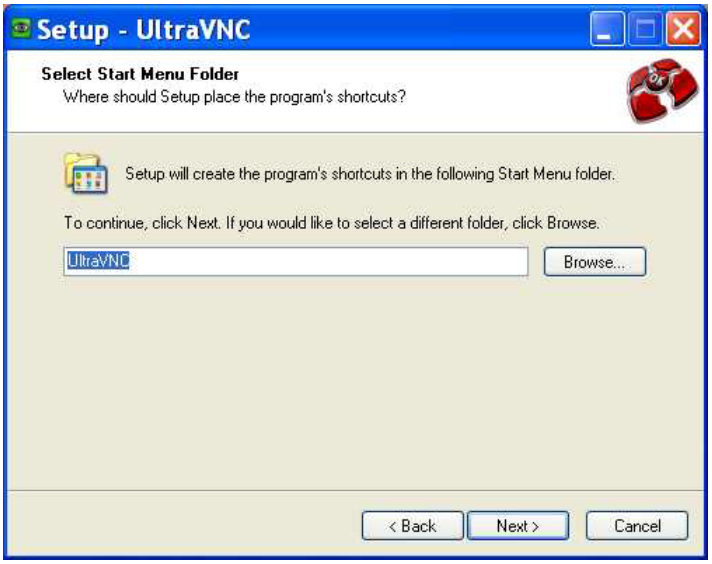


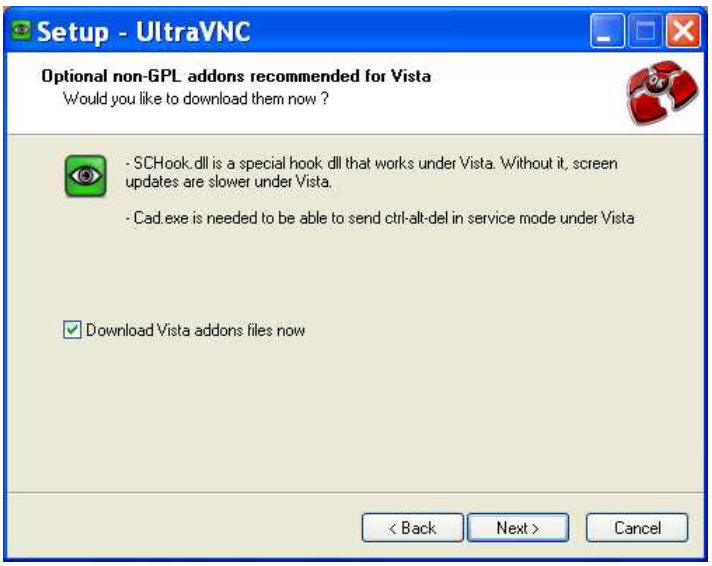


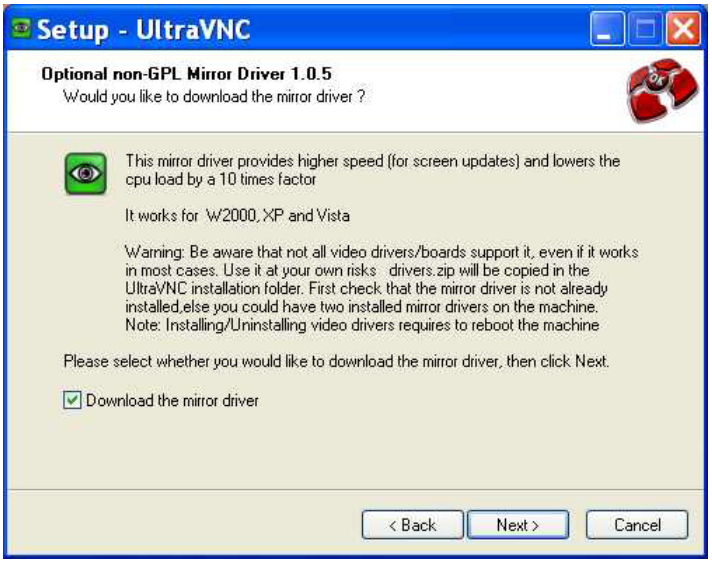

Setup - UltraVNC
Information
Please read the following important information before continuing.
When you are ready to continue with Setup, click Next.
* Ultr@VNC - Latest modifications
**v1.0.6.3
viewer
+gui lock while reconnect fixed
+removed flasher (not used codepart)
+tab order fixed
+crash on exit fix
+fix cursor and scaling
server
+fix unload video driver and xp64
< Back
Next >
Cancel


Setup - UltraVNC
Select Destination Location
Where should UltraVNC be installed?
Setup will install UltraVNC into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Program Files\UltraVNC
Browse...
At least 2,4 MB of free disk space is required.
< Back
Next >
Cancel

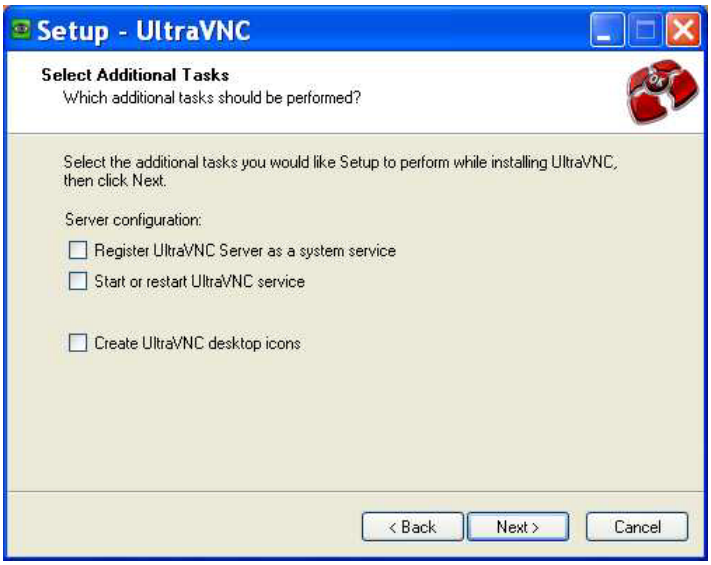

Setup - UltraVNC
Select Components
Which components should be installed?
Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.
Full installation
Full installation
UltraVNC Server Only
UltraVNC Server Only "silent"
UltraVNC Viewer Only
< Back
Next >
Cancel


Setup - UltraVNC
Select Start Menu Folder
Where should Setup place the program's shortcuts?
Setup will create the program's shortcuts in the following Start Menu folder.
To continue, click Next. If you would like to select a different folder, click Browse.
UltraVNC
Browse...
< Back
Next >
Cancel

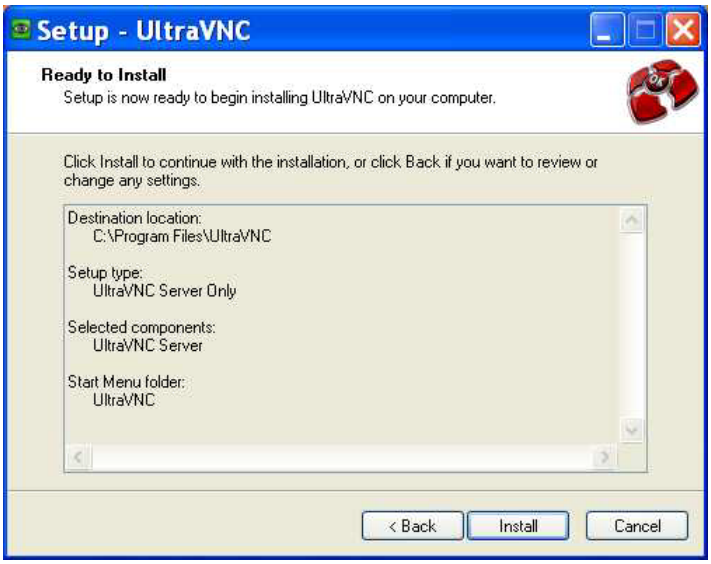

Setup - UltraVNC
Optional non-GPL addons recommended for Vista
Would you like to download them now ?
- SCHook.dll is a special hook dll that works under Vista. Without it, screen updates are slower under Vista.
- Cad.exe is needed to be able to send ctrl-alt-del in service mode under Vista
Download Vista addons files now
< Back
Next >
Cancel


Setup - UltraVNC
Optional non-GPL Mirror Driver 1.0.5
Would you like to download the mirror driver ?
This mirror driver provides higher speed (for screen updates) and lowers the cpu load by a 10 times factor
It works for W2000, XP and Vista
Warning: Be aware that not all video drivers/boards support it, even if it works in most cases. Use it at your own risks drivers.zip will be copied in the UltraVNC installation folder. First check that the mirror driver is not already installed,else you could have two installed mirror drivers on the machine.
Note: Installing/Uninstalling video drivers requires to reboot the machine
Please select whether you would like to download the mirror driver, then click Next.
Download the mirror driver
< Back
Next >
Cancel

Mirror driver only get downloaded, NOT installed. This need to be done manual.



For first time install you best don't register it as service, this can always be done later from the winvnc systray. First test if it works, and then register as service when needed.



1.1.1 Automate Installation

If you need to install UltraVNC on a large number of computers, you might consider automating the installation.

The following command line parameters can be passed to the setup:
`/dir="Dirname"`
Sets installation directory to *Dirname*.
`/no restart`
Suppresses a reboot at the end of the installation.
Not required since the installation no longer requires are boot.
`/silent` or `/very silent`
Suppresses either pop-up of dialog boxes or any GUI at all.

`/loadinf="Filename"`
Loads the configuration file *Filename*for the installation.
This configuration file can be generated by going through setup with `UltraVNC-xxxx-Setup.exe /saveinf="Filename"`.
`Filename` should be fully qualified.
`/log`
Writes a log file to the Temp directory.
Could be used for debugging.

1.2 UltraVNC Mirror driver

1.2.1 How does it Work?

The Mirror Video Driver is a driver that UltraVNC (for instance) can use to be quickly and efficiently notified with screen changes. Using it on an UltraVNC server results in a excellent accuracy. The video driver also makes a direct link between the video driver frammebuffer memory and UltraWinVNC server. Using the framebuffer directly eliminates the use of the CPU for intensive screen blitting, resulting in a big speed boost and very low CPU load.

1.2.2 Supported OS for mv2 mirror driver?

win 2000
win 2003
win 2008
XP
Vista
Win 7

1.2.3 Installation

If you have a previous version installed, it is recommended to uninstall it first, by doing the following:
setupdrv.exe uninstall
Installation is done by setupdrv.exe install
The program setupdrv.exe is located in the folder you've chosen during the driver installation.

1.2.4 Manual Uninstall

net stop vnccom (stop communication manager service) Driver mv2 doesn't use the vnccom , only needed with the old drivers
Under XP: Control Panel ⇒ System ⇒ Hardware ⇒ Device Manager ⇒ Display Adapters ⇒ Uninstall mirror driver.
Under W2000: W2000 does not allow video drivers to be removed while running.
Trick: Remove vncdrv.sys (that is in system32/drivers), and reboot. You now can remove the driver the same way as with XP, via the device manager.

1.2.5 Upgrading issue

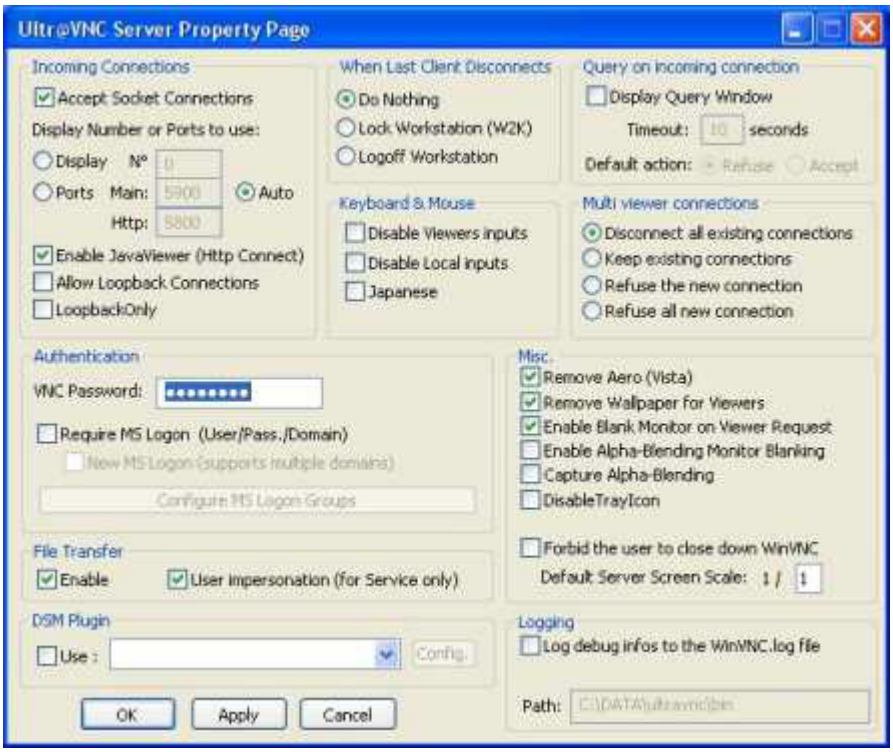
For each version the vncdrv.sys and vnccom.sys are a pair. Vncdrv.sys is a kernel driver, so can only be unloaded on reboot. After upgrading the driver, vncdrv.sys is still the old version, but vnccom.sys is already the new one. Switching of vncdrv.sys is done on reboot. Don't use the driver before you reboot.

2 First Run

2.1 First Server Run

If you run ultravnc server for the first time, the settings "ultravnc.ini file" does not exist and firewall need to allow winvnc.

When no password has been set, ultravnc prompt you to set one.

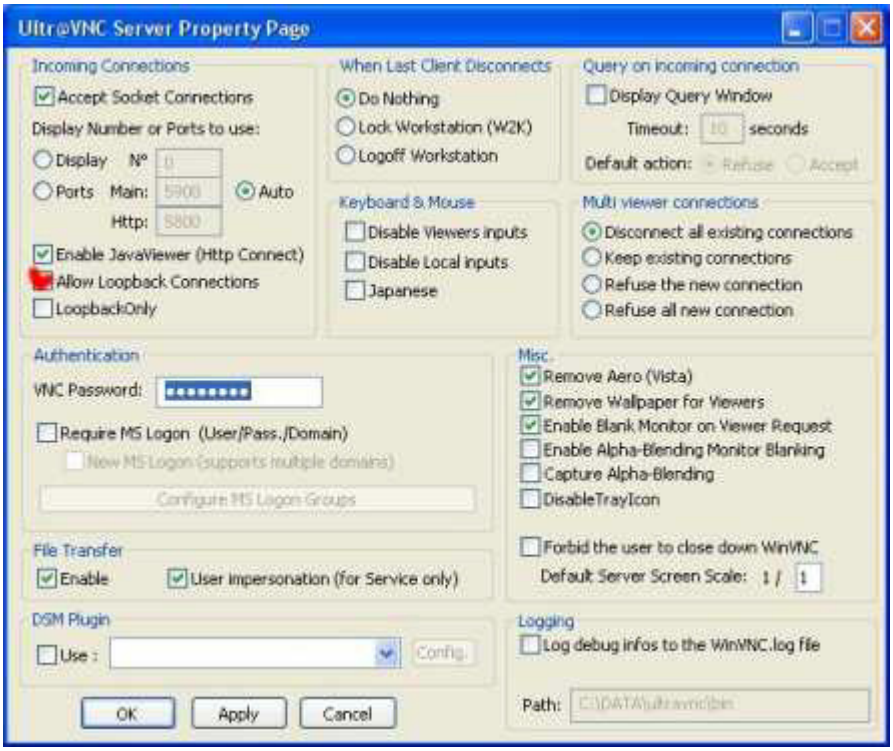


When you are running on XP and winvnc was installed as service you first get the "runas" box, DON'T FORGET TO UNCHECK else you tell runas that winvnc can't make changes to a file.

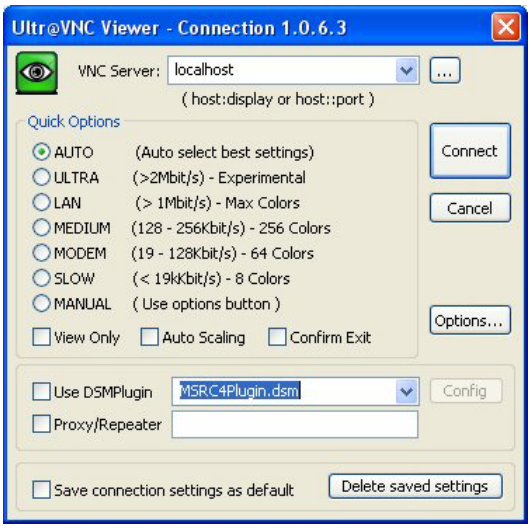
2.2 First connection (loopback)

Now that the server is running, we can make a fast test connection in loopbackmode.(loopback mode= server+ viewer on same PC)

1* Tell server to allow loopback 



2* Tell viewer to connect to the server
Start the viewer vncviewer.exe

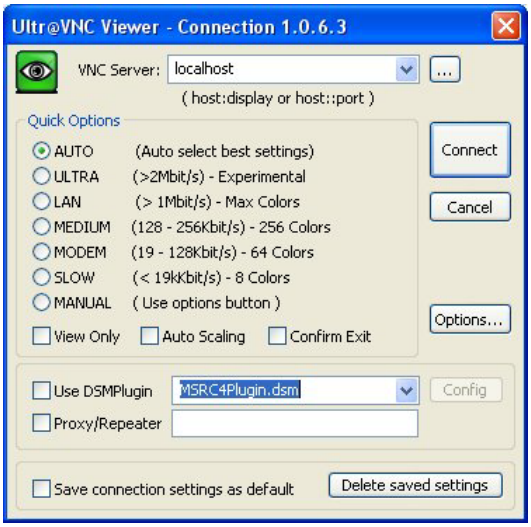


When all is ok you should see the viewer showing himself like watching 2 mirrors(not usufull to do anything, but it tell server and viewer can connect)

2.3 First connection (local network)

Install viewer on second PC (the pc you gonna use the control the server)
* Use the installer and select viewer only.
* Or, copy vncviewer.exe on a usb stick and plug this in your viewer PC.
* Or, use a shared/mapped folder and copy.

The **server ip address** can be found by hovering the mouse over the vnc server tray icon.
Instead of "localhost" you need to enter this ip address.



3 Internet Connection

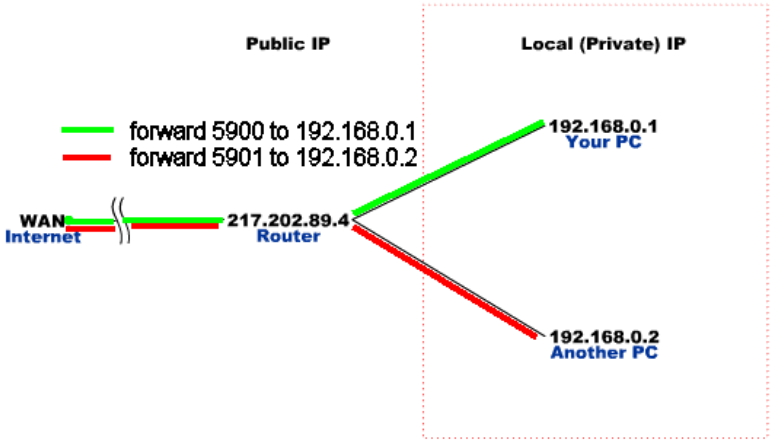
We only handle 2 cases
A. Server has a official ip address
B. Server has a local ip and use a Nat router to connect to the internet. The router has the official ip address.
The way you connect is independed of the viewer ip address (local, official)

A. Server has a official ip address
When the server has an official ip address there is no difference between a LAN or internet connection. You need to enter the server ip in the viewer connection box. (see last part "First Run")

B. Server has a private ip and use a Nat router to connect to the internet. The router has the official ip address.
The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets (local networks):

10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

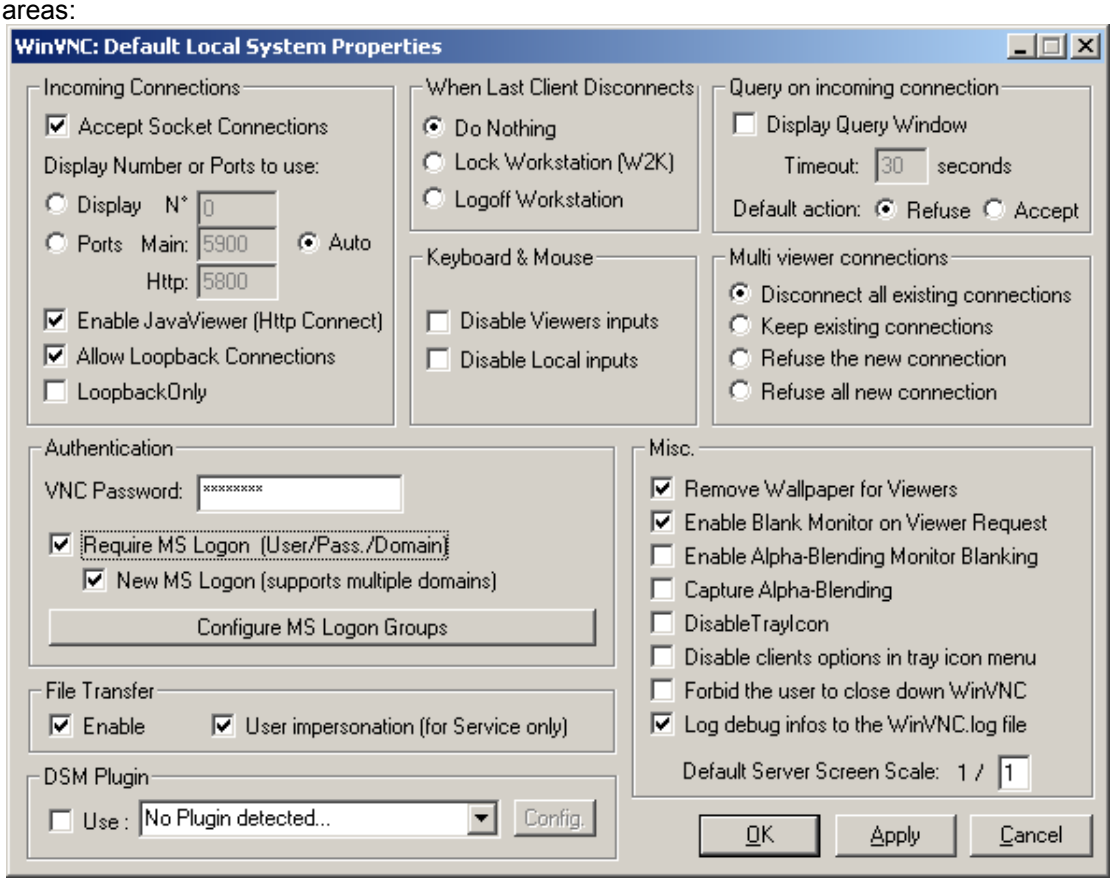
If your server has an ip address that's in one of the above ranges you are using some nat router to connect to the internet and the viewer can not make a direct connection to the server.
The solution is tell the nat router that he need to send a port to your local pc , the viewer connect to the nat router ip address.
Sample:



4 UltraVnc Configuration

4.1 Admin Properties

The "Admin Properties" menu item in the system tray UltraVNC icon menu refers to Default Local System Properties (service mode) or Current User Properties (application mode) and allows for customizing several areas:



4.2 Configurations

Incoming connections

Accept Socket Connections
Should be activated for normal operation. The display number and ports to use can be configured or set to Auto which defaults to Display 0, Port 5900and JavaViewer port 5800.
The port is always Display No + 5900.

Display
Defaults to 0.

Ports
Defaults to 5900 and 5800 for HTTP.

Enable JavaViewer (HTTP connect)
Allows to view a remote computer by opening a browser and go to http://*remote-machine*:*http-port*/

Allow Loopback Connections
Sometimes this could be helpful for tests. Normally it's not needed since the result is not very useful.

Loopback Only
Needed for tests. Connections from outside are not allowed.

When last client disconnects

In a helpdesk scenario, you normally "Do Nothing" when disconnecting. When administering servers via remote control, you might wish to either "Lock Workstation" or "Logoff Workstation" for security reasons.

Query on incoming connection

If enabled, every time someone tries to connect via UltraVNC, a pop-up dialog informs the user and asks the user to either accept or refuse the attempt. Configure the timeout for the dialog window and what action should be taken if the user clicked no button until timeout.

Keyboard & Mouse

Some situations (e.g. presentations) require that either the viewer or the remote computer don't input keyboard or mouse events. This can be configured by "Disable Viewer inputs" or "Disable Local inputs".

Multi viewer connections

Here you can configure the behavior if multiple viewers attempt to connect to the same UltraVNC server. "Disconnect all existing connections" implies that only one viewer can be connected at a time and the last one wins. "Keep existing connections" allows for several viewers simultaneously. "Refuse the new connection" implies that only one viewer can be connected at a time and the first one wins. "Refuse all new connections" ??

Authentication

"VNC Password" is a per-machine password and is required.

Require MS Logon

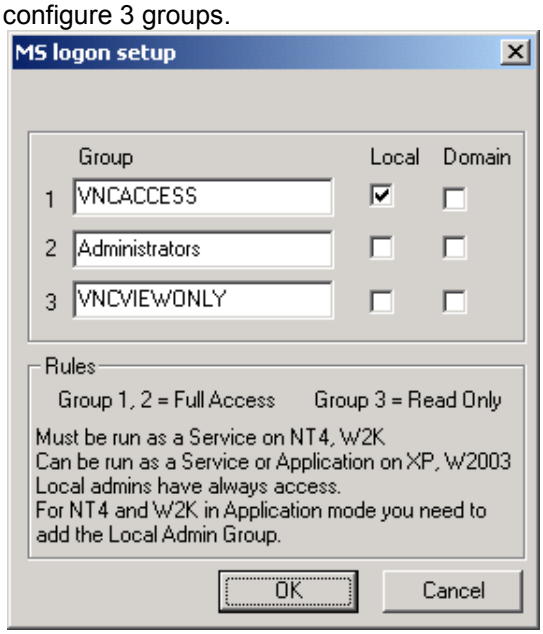
Activates MS-Logon I. Works on Windows 9x as well as Windows NT4/2000/XP. Requires computer and user to be in the same domain.

New MS Logon

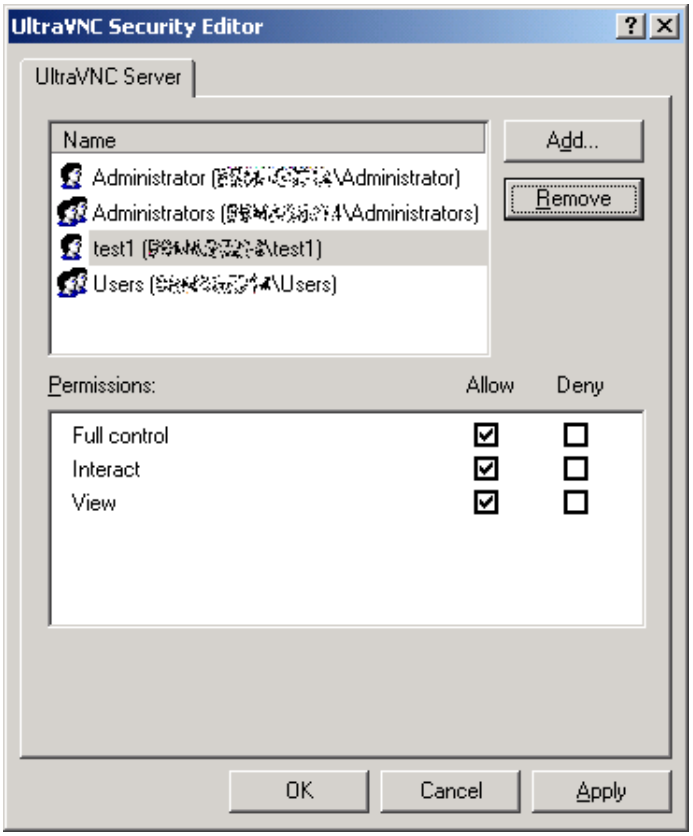
Activates MS-Logon II. Allows for cross-domain authentication, i.e. computer is in domain A, user in domain B with a trust between A and B (typically in Active Directory). Works only on Windows NT4/2000/XP.

Configure MS Logon Groups

Opens the configuration dialog for MS-Logon authorization. For MS-Logon I there is a dialog allowing to configure 3 groups.



For MS-Logon II there is the standard Windows Security property page.



DSM Plugin

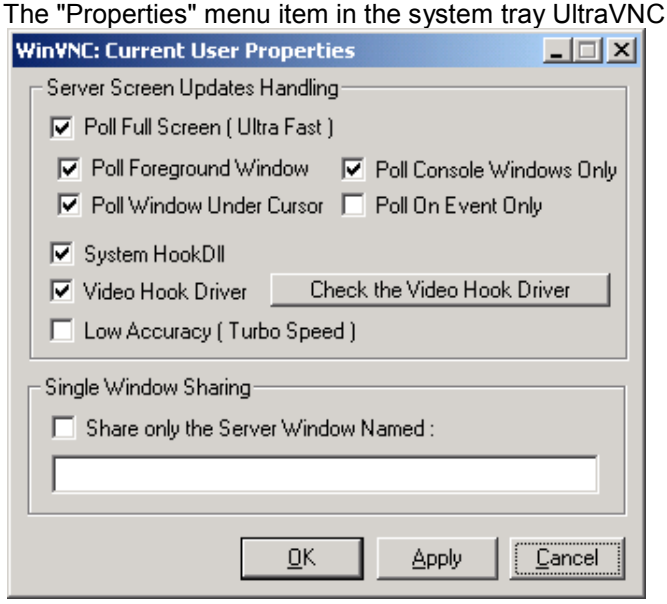
If there are any DSM (Data Stream Modification) Plugins available, their usage can be configured here. Currently there are several encryption plugins available.

Miscellaneous

Remove Wallpaper for Viewers
To reduce network traffic the wallpaper on the remote computer's desktop can be removed during the connection.
Enable Blank Monitor on Viewer Request
Allow viewers to disable the monitor if they request so.
Enable File Transfer
Enable the UltraVNC File Transfer.
Log debug info to the WinVNC.log file
Enable logging. The log file is in C:\WinNT\system32 if winvnc runs as service. The logging level can be configured in the registry.
Disable Tray icon
The icon in the system tray can be disabled to disallow users to change any settings.
Forbid the user to close down WinVNC
Disallow users to close down WinVNC.
Disable clients options in tray icon menu
Disable the "Properties" menu item in the system tray icon menu.
Capture Alpha-Blending
??
Enable Alpha-Blending Screen Blanking
Enable another method to disable the monitor.
Default Server Screen Scale
The server screen can be scaled down here.

4.3 Properties

The "Properties" menu item in the system tray UltraVNC icon menu refers to per user settings.



Poll Full Screen

??

Poll Foreground Window

??

Poll Console Windows Only

??

Poll Window Under Cursor

??

Poll On Event Only

??

System Hook Dll

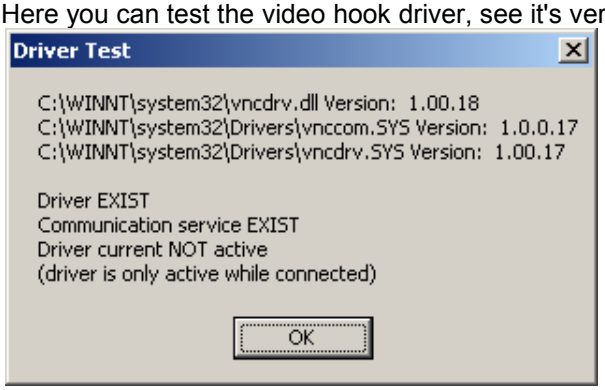
Provides DDI hooking, especially on Windows 9x.

Video Hook Driver

The video hook driver provides high speed and low CPU load on Windows 2000/XP/2003.

Check the Video Hook Driver

Here you can test the video hook driver, see it's version and whether it's currently active.



Low Accuracy

Get higher speed with reduced accuracy.

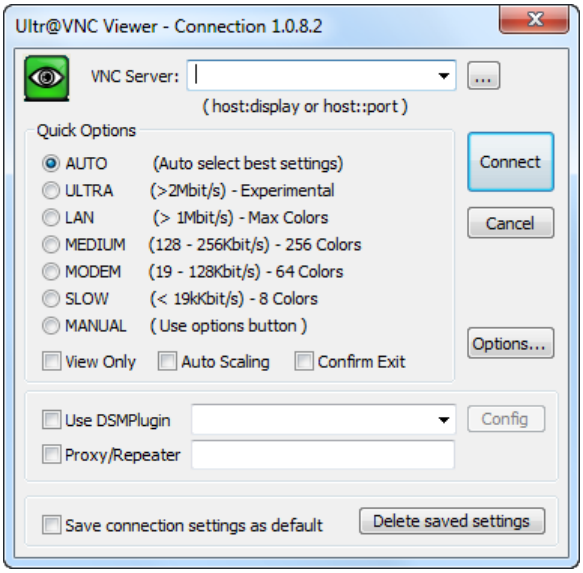
Share only the Server Window Named

Do not share the whole desktop but only the window with the specified name.

5 UltraVnc Viewer Configuration

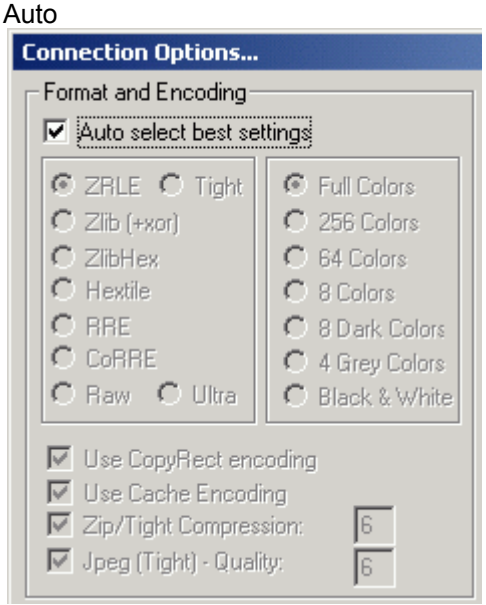
5.1 Ultra Viewer Configuration

There are a lot of options that can be configured from the viewer side.

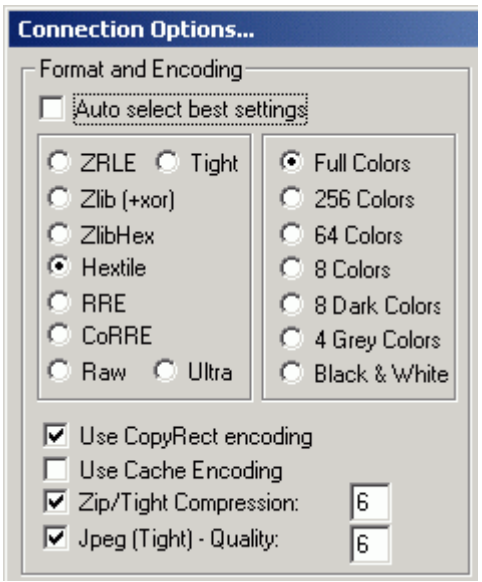


Quick options
The quick options relate to the following configurationsettings:

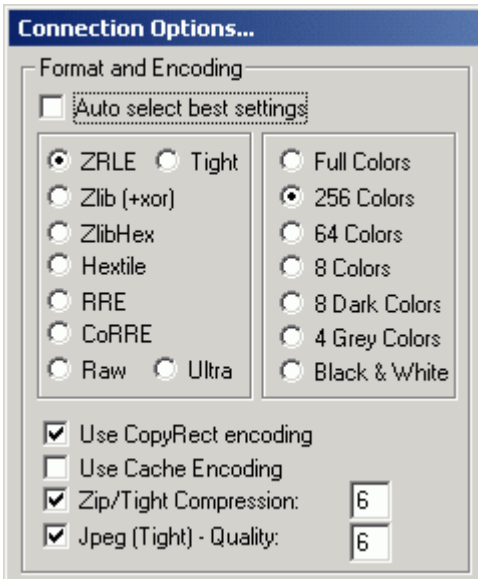
Auto



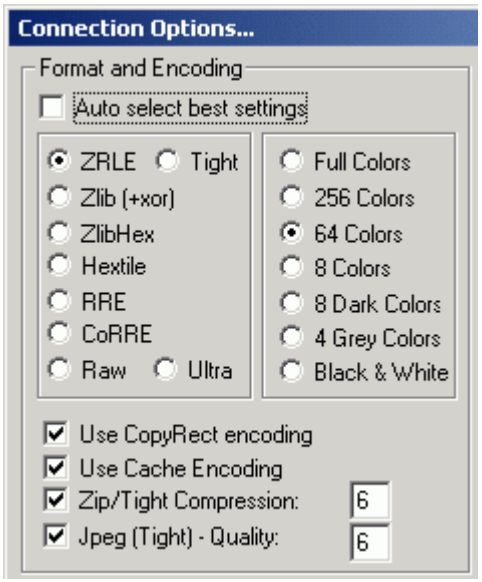
LAN



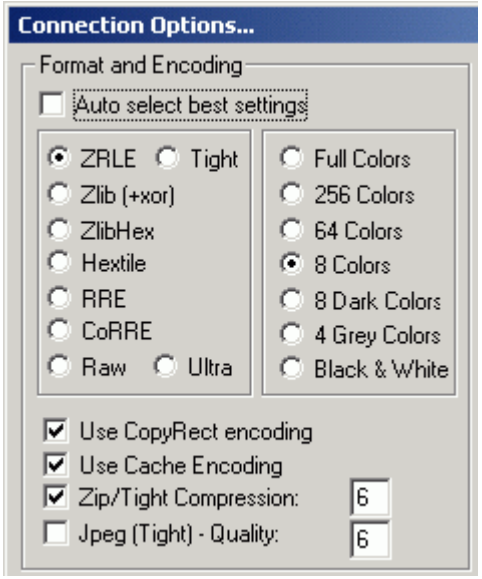
Medium



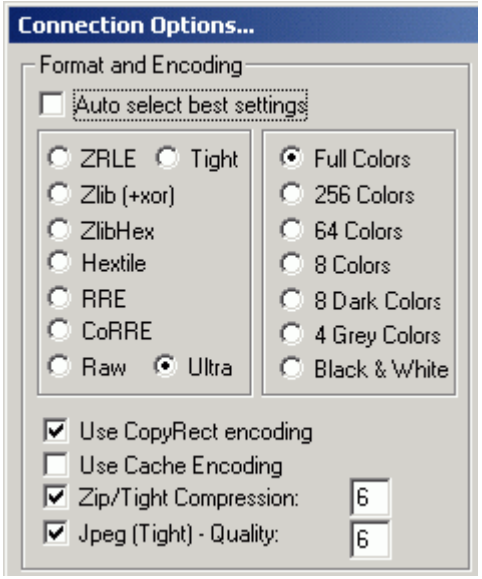
Modem



Slow



Ultra



View Only
No keyboard or mouse events are sent from the viewer to theserver. The server screen can only be viewed, but notcontrolled.

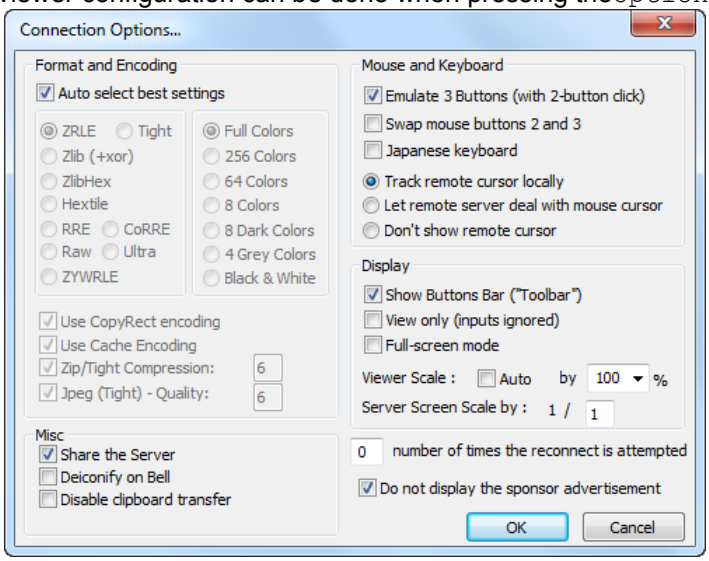
Auto scaling
The viewer window is automatically scaled to fit the size ofyour local screen.

Use DSM Plugin
Choose a DSM (Data Stream Modification) Plugin and configureit.
To use an encryption plugin, for instance, check this option andselect the plugin in the combo box. The plugin file must be inthe same directory than the vncviewer.exe program. And of course,the same plugin must be used by the UltraVNC server you connectto.

Proxy/Repeater
Specify the repeateraddress here.

Save connection settings as default
If checked, the current settings are saved as default optionsin a configuration file. So next time you run the viewer, youdon't have to reselect all your favorite settings.

Further viewer configuration can be done when pressing the`Options` button.



Format and Encoding
See Encodings section below.
Note: Grey colors only works with 32 bits color screenresolution. 16/24 bits color resolutions just don't work withgrey colors.
Mouse buttons

Mouse cursor

Display

Show Buttons Bar
Show the toolbar after connection is estabilished, or hide the toolbar (not vinked).
View only
Start connection in view only mode, all inputs are ignored by the server.
Full-screen mode
Start connection in full screen mode.
Viewer scale
Scaling on the viewer side, select a pre-defined scaling option. Or use ‘Auto’ to preserve the client desktop inside your own desktop.

Miscellaneous

[0] number of time the reconnect is attempted
0 (default), never reconnect
9 (maximum) 9 time trying reconnect.
gui reconnectnumber only for now.
This is the number of times a reconnect is made before the viewer close the connection.

5.1.1 Encodings

This section (except Ultra encoding) is taken from[TightVNC'svncviewer man page](#).

The server supplies information in whatever format is desiredby the client, in order to make the client as easy as possible toimplement. If the client represents itself as able to usemultiple formats, the server will choose one.

Pixel format refers to the representation of anindividual pixel. The most common formats are 24 and 16 bit"true-color" values, and 8-bit "color map" representations, wherean arbitrary map converts the color number to RGB values.

Encoding refers to how a rectangle of pixels are sent(all pixel information in VNC is sent as rectangles). Allrectangles come with a header giving the location and size of therectangle and an encoding type used by the data which follows.These types are listed below.

Raw
: The raw encoding simply sends width*height pixel values. Allclients are required to support this encoding type. Raw is alsothe fastest when the server and viewer are on the same machine,as the connection speed is essentially infinite and raw encodingminimizes processing time.

CopyRect
: The Copy Rectangle encoding is efficient when something isbeing moved; the only data sent is the location of a rectanglefrom which data should be copied to the current location.Copyrect could also be used to efficiently transmit a repeatedpattern.

RRE
: The Rise-and-Run-length-Encoding is basically a 2D version ofrun-length encoding (RLE). In this encoding, a sequence ofidentical pixels are compressed to a single value and repeatcount. In VNC, this is implemented with a background color, andthen specifications of an arbitrary number of sub rectangles andcolor for each. This is an efficient encoding for large blocks ofconstant color.

CoRRE
: This is a minor variation on RRE, using a maximum of 255x255pixel rectangles. This allows for single-byte values to be used,reducing packet size. This is in general more efficient, becausethe savings from sending 1-byte values generally outweighs thelosses from the (relatively rare) cases where very large regionsare painted the same color.

Hextile
: Here, rectangles are split up in to 16x16 tiles, which aresent in a predetermined order. The data within the tiles is senteither raw or as a variant on RRE. Hextile encoding is usuallythe best choice for using in high-speed network environments(e.g. Ethernet local-area networks).

Zlib
: Zlib is a very simple encoding that uses zlib library tocompress raw pixel data. This encoding achieves good compression,but consumes a lot of CPU time. Support for this encoding isprovided for compatibility with VNC servers that might notunderstand Tight encoding which is more efficient than Zlib innearly all real-life situations.

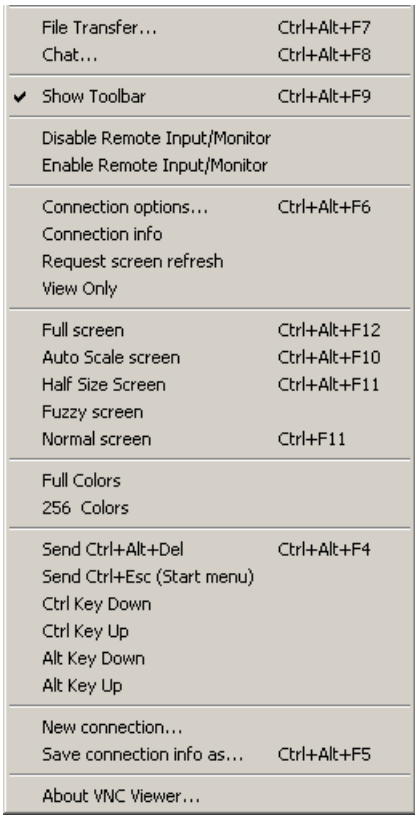
Tight
: Like Zlib encoding, Tight encoding uses zlib library tocompress the pixel data, but it pre-processes data to maximizecompression ratios, and to minimize CPU usage on compression.Also, JPEG compression may be used to encode color-rich screenareas (see the description of -quality and -nojpeg optionsabove). Tight encoding is usually the best choice forlow-bandwidth network environments (e.g. slow modemconnections).

Ultra
: Experimental, Ultra encoding provides real time performanceover a LAN by utilizing LZO compression. LZO is a datacompression scheme which is suitable for data de-/compression inreal-time. This means it favors speed over compressionratio.

5.2 VNCViewer Toolbar

- Send CTRL+ALT+DEL
- Toggle Full Screen Mode
- Show Connection Options...
- Refresh Screen
- Send 'Start' (CTRL+ESC) to host
- Send Custom Key
- Show Status Window
- Close Connection
- Hide Toolbar Buttons
- Toggle Remote Input and Remote Blank Monitor
- Open File Transfer...
- Select Single Window
- Select Full Desktop
- Open Chat...

5.3 VNCViewer Context Menu



File Transfer... (Hotkey `CTRL+ALT+F7`)

Open the file transfer dialog window.

Chat... (Hotkey `CTRL+ALT+F8`)

Open the chat dialog window.

Show/Hide Toolbar (Hotkey `CTRL+ALT+F9`)

Show or hide the VNCViewer toolbar.

Disable/Enable Remote Input and Monitor

Disable keyboard and mouse input as well as the monitor on the remote computer.

Connection options... (Hotkey `CTRL+ALT+F6`)

Open the connection option dialog window.

Connection info

Open the connection info window.

Request screen refresh

Redraw the screen in VNCViewer. Sometimes the display in VNCViewer misses updates or becomes corrupted. A screen refresh can then insure that VNCViewer's display and remote computer's display are in sync.

View only

Disables sending mouse and keyboard events from the VNCViewer to the remote computer.

Various screen size options

 Full screen mode (hotkey `CTRL+ALT+F12`) displays the remote screen on the entire screen of your display.
Together with a hidden toolbar this feels like sitting in front of the remote computer.
Scaled viewer mode displays the scaled remote screen in a window with a user defined size.
Scaled server mode generates less network traffic from server side and uses a pixel blending algorithm to optimize the display.
Fuzzy screen mode combines Server and Viewer scaling to provide reasonable visual comfort and speed even over very slow connections.
Auto scaling mode scales the view to fit the viewer screen. Normal screen mode (hotkey `CTRL+F11`) displays the remote screen 1:1.

Full/256 Colors


Change the color depth of the screen.

Send various key combinations


Send `CTRL+ALT+DEL` (hotkey `CTRL+ALT+F4`), `CTRL+ESC` (this opens the start menu), `CTRL+Key Down`, `CTRL+Key Up`, `ALT+Key Down` or `ALT+Key Up`.

New connection...
Start a new connection.

Save connection info as... (Hotkey `CTRL+ALT+F5`)
Save the options and settings of the active connection in a file.

About VNC Viewer...
See version and licensing information of VNCViewer.

5.4 Additional Hotkeys

Pressing ALT or CTRL send ALT/CTRL directly to the VNCServer, as if the user selected "CTRL DOWN/CTRL UP/ALT DOWN/ALT UP" from the system menu.

When SCROLL-LOCK is activated, all key combinations (except CTRL+ALT+DEL) are directly sent to the remote computer:

- Instead of switching applications on the client side, ALT+TAB is sent to the VNCServer.
- Instead of opening the start menu on the client side, CTRL+ESC is sent to the VNCServer.
- Instead of opening the system menu on the client side, ALT+SPACE is sent to the VNCServer.
- Pressing Break/Pause key toggles Full-Screen mode on or off.
- Pressing PRINT-Screen key requests a full screen update (same as selecting "Request Screen Refresh" from the system menu)

All the above can be disabled by turning the SCROLL-LOCK key off.

5.5 UltraVnc File Transfer

Ultr@VNC features an embedded File Transfer with intuitive Graphical User Interface allowing for easy file copy between local and remote computers.

- Compression: Files are compressed on the fly during transfers, ensuring optimal bandwidth utilization
- Resume: Interrupted transfers can be resumed, thus only the missing parts of the files are resent
- Delta Transfer: only the changed parts of the files are resent

- Transfers are asynchronous if wanted:
  - When the File transfer GUI Window is visible there are no screen updates, so the speed for file transfers is max.
  - When File transfer GUI Window is minimized screen updates and file transfers occur in parallel.
- Display of progress percentage during transfers
- Directory Transfer
- Uses the current Ultr@VNC connection
- Optional User Impersonation option, limiting remote file system access to identified Windows ™ users only

6 UltraVnc Java Viewer

UltraVNC server features a JavaViewer Applet that allows for remote control without a any viewer application installed !

All you have to do is open a Web Browser (with Java ™ installed) and connect to `http://remote computer:5800/`

(`remote computer` is either the (DNS) name or the IP address of the remote computer to be controlled)

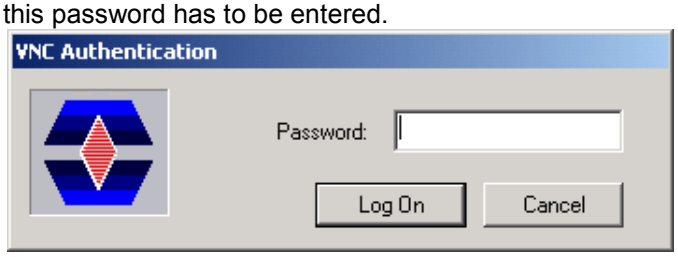
- Supports **File transfer** (same kind of GUI than in win32 Viewer, but simpler). It makes possible files transfers from virtually any OS supporting Java (Linux, Mac OS...) to Ultr@VNC servers running under Windows ™.
  Since this requires the JavaViewer to access the viewing machine's hard drive, you are prompted for an "UltraVNC" signed applet certificate acceptance. As this applet is injected in your Web browser by the Ultr@VNC server you are accessing to, if you trust the server, you can trust the applet.
- Supports **MS Logon**authentication method.
- Supports various **color modes** (from 8 colors to full colors) and **compression methods**, for optimal performances over slow (internet/modem) connections

7 UltraVnc Authentication

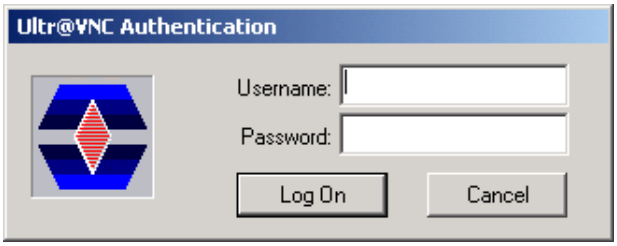
Currently there are three different authentication methods available for UltraVNC:

- Classic VNC Authentication
- MS-Logon I
- MS-Logon II

Classic VNC authentication stores a password on the remote machine. When connecting with the viewer, this password has to be entered.



Both MS-Logon methods rely on Microsoft Windows Logon authentication, i. e. username and password of a Windows domain or machine account is used for authentication.



MS-Logon I restricts the user accounts to be in the same domain than the machine account, but is available on Windows 9x.
MS-Logon II allows for cross-domain authentication, but only works on Windows NT, 2000, XP and 2003.

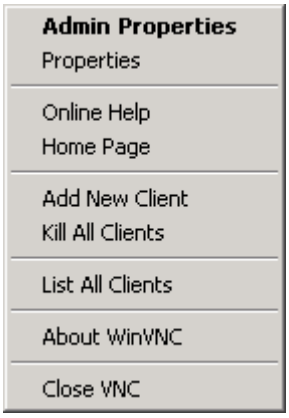
7.1 Classic VNC Authentication

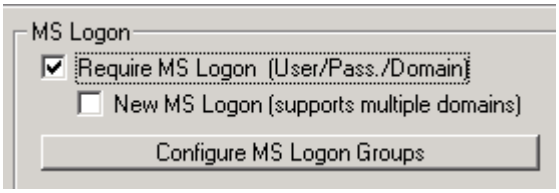
Classic VNC Authentication allows a single password of up to 8 characters to be stored by VNC Server, which remote users must supply when prompted in order to authenticate.

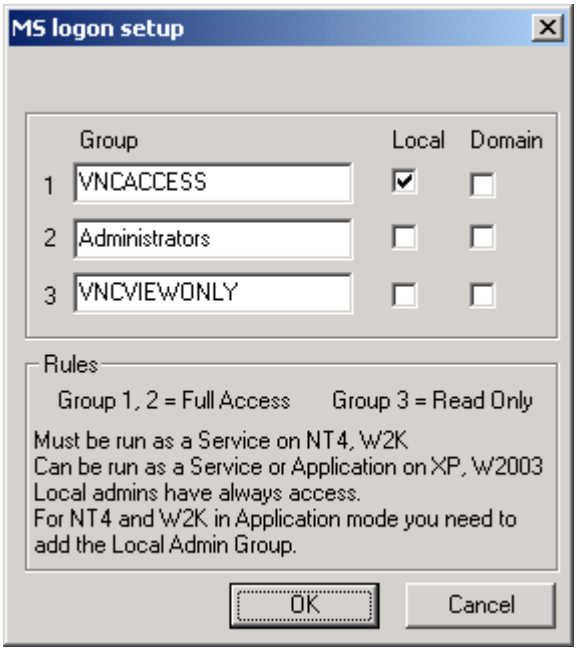
7.2 MS-Logon I

With UltraVNC the WinVNC Server access can be managed using MS Users, Domains and Groups available from the machine that is hosting this WinVNC server. Currently, NT domains and active directories are supported. Child domains are NOT supported, user has to belong to the server's domain.

Right click the WinVNC icon in the System Tray and choose "Admin Properties".







In the Admin Properties page check "Require MS-Logon".

Then click on "Configure MS Logon Groups".
Here you can add or remove users and groups or change their rights.

A few things must be known and configured if you want this functionality to work fine on your WinVNC Server machine, and it depends on the version of Windows that is used.

To use MS Logon under Windows 95, Windows 98, and Windows Millennium Edition, you also have to enable the NTLM security services by opening Control Panel, Network, Access Control, and then selecting User-level access control. Win 9.x require 2 dlls radmin32.dll and rlocal32.dll this can be found in the nexus.exe.

Under Windows XP, the ForceGuest registry value is set to 1 by default in the following registry key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

On a Windows XP computer you must check:
If the Guest account is enabled, an SSPI logon will succeed as Guest for any user credentials.
If ForceGuest is disabled (set to 0), SSPI will log on as the specified user.
If the authtest util gives guest account blocked, an open guest account is detected and ms logon denies all access.

7.3 MS-Logon II

7.3.1 Description

In addition to the first implementation of MS-Logon (MS-Logon I), MS-Logon II is able to do cross-domain authentication, i.e. the user account can be in another domain than the computer account.

Supports

- Windows NT, Windows 2000, Windows XP and Windows 2003.
- Any possible nesting of groups and users.
- Different naming styles:

- domain\user
- user@domain.com (UPN, i.e. User Principal Name)

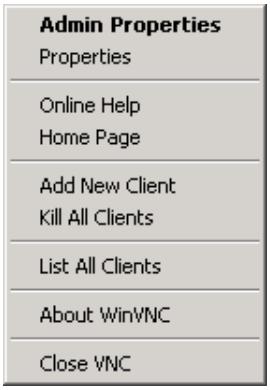
7.3.2 Requirements

- On Windows NT 4, you need at least SP4 and the security configuration manager installed.
- Under Windows XP, the `ForceGuest` registry value is set to `1` by default in the following registry key:
  `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`
  If the Guest account is enabled, an SSPI logon will succeed as Guest for any user credentials.
  If `ForceGuest` is disabled (set to `0`), SSPI will log on as the specified user.
  So it's important to disable `ForceGuest`. Otherwise all authorization is done against the guest account!
- Policy Settings: Authentication will fail if "Deny logon to the computer from the network" is enabled for a group the logon account is a member of. This applies to both Local Policy Settings as well as Group Policy Objects.
  So make sure user accounts used for MS Logon authentication are not affected by these settings.

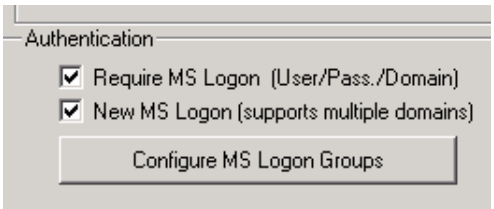
7.3.3 Configuration

7.3.3.1 Manual configuration

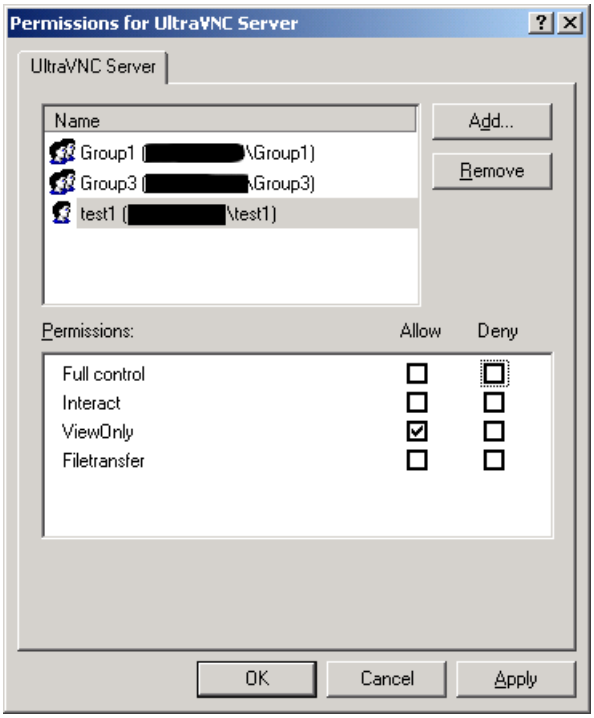
Right click the WinVNC icon in the System Tray and choose "Admin Properties".



In the Admin Properties page check "Require MS-Logon" and "New MS-Logon".



Then click on "Configure MS Logon Groups".
Here you can add or remove users and groups or change their rights.



`Interact` is the normal mode where you can take over mouse and keyboard. It's a synonym for `Full Control`.
`View only` allows the account to view the remote screen, but local mouse and keyboard cannot control the remote screen.

7.3.3.2 Automated configuration

You can use the MSLogonACL tool to export the ACL from one machine and import it to another.

7.3.4 To be tested

Since MSLogon II is relatively new and there are various different scenarios how to use it, we encourage everybody to share their experience. Please post your results to the UltraVNC MS-Logon forum.
There are a number of factors which are to be considered: Different OS versions, if Active Directory is used or old-style NT trusts, whether local or domain based accounts are used, the naming convention which is used and various possible nesting of groups.

OS
: WinNT, W2K, wXP, W2K3

Infrastructure
: With/without Active Directory

Accounts
: Local and/or domain users/groups

Naming styles
: user, machine\user, domain\user, user@domain.com (UPN), group, domain\group

Domains
: (implies trusts/AD) user and/or group in other domains than computer, nested groups over multiple domains

8 UltraVnc Command line Parameters

8.1 WinVNC

8.1.1 Running WinVNC

`-service`
Runs WinVNC as a service.

`-servicehelper`
Runs the WinVNC Service Helper app, i.e. the systray icon.

`-run`
WinVNC is being run as a user-level program.

8.1.2 Installing WinVNC as Windows service

`-install`
Installs WinVNC as a service.

`-sinstall`
Installs WinVNC as a service silently, i.e. no message box appears.

`-remove`
Removes the WinVNC service.

`-reinstall`
Silently removes WinVNC service, then re-installs it.

8.1.3 Accessing various Configuration Options

`-settings`
Shows the Properties dialog of an existing instance of WinVNC.

`-defaultsettings`
Show the Admin Properties dialog of an existing instance of WinVNC.

`-multi`
WinVNC is being run as a user-level program. Multiple simultaneous instances are allowed.

`-fus`
WinVNC is being run as a user-level program. Warning about multiple instances is disabled.

`-about`
Shows the About dialog of an existing instance of WinVNC.

`-help`

8.1.4 Connecting VNCViewers

`-connect` *`host[:display]`*
Adds a new client to an existing copy of winvnc.
Needs the computer name (DNS name) or IP address and optionally the display number (separated from the host name with a colon (:).

`-connect` *`host[::port]`*
Adds a new client to an existing copy of winvnc.
Needs the computer name (DNS name) or IP address and optionally the port number (separated from the host name with two colons (::).

`-autoreconnect`
Is used in conjunction with the `-connect` switch when having a server "back-connect" to a listening viewer. You can use it in a batch file for your clients that are behind a firewall that is not under your control. The batch file looks something like this:
`"c:\program files\ultravnc\winvnc" -autoreconnect -connect 12.34.56.78`
On the local computer run the viewer in "listening" mode, and have someone on the server end run the batch file. The `-autoreconnect` will make the server end attempt to reconnect to the listening viewer if the connection drops or is closed. It will immediately reconnect to the listening viewer if the session is closed. Close the listening viewer altogether in order to stop the server end from "autoreconnecting" to your computer. The server attempts to "autoreconnect" for only a few seconds. Note that this "autoreconnect" param *must be before* the "connect" one on the command line!

`-kill`
: Kills any already running copy of WinVNC.

8.2 WinVNC SingleClick

In addition to the normal WinVNC command line parameters, WinVNC SC supports the following parameters:

`-id` *number*
: Used with the repeater in mode II. Specifies a number to identify the session. In the `-connect` parameter use the repeater's name or IP address (and the repeater's port) instead of the remote host name.

`-plugin` *plugin*
: Use the specified DSM plugin.

`-noregistry`
: Don't store SingleClick DSM settings in the registry. Used in conjunction with the -plugin parameter.

`-notrayicon`
: Do not display the UltraVNC icon in the system tray.

`-read only`
: Don't send keyboard and mouse events to the remote computer.

`-username` *username*
: Use the specified username.

`-password` *password*
: Use the specified password.

8.3 VNCviewer

VNCViewer supports numerous command line parameters which allow for configuration of nearly every aspect of the viewer.

`-help`, `-?` or `-h`
: Print a help message.

`-listen` *[port]*
: Start the VNCviewer in listen mode. If `port` is specified, the viewer listens on that port instead of ???.

`-restricted`
: ???

`-viewonly`
: Do not send local keyboard or mouse events to the remote computer.

`-nostatus`
: Don't show the status window while connecting.

`-nohotkeys`
: Do not enable hot keys (like `CTRL+ALT+F9` for full screen mode etc.). Can be useful in case of conflict with other installed software hotkeys.

`-notoolbar`
: Do not display the toolbar.

`-autoscaling`
: Automatically scale the viewer window so that the remote screen fits at best your local screen size.

`-fullscreen`
: Display viewer in full screen mode.

`-noauto`
: Disable auto mode. Required for using the color options below or saving a custom configuration (otherwise the settings from quick options always override).

`-8bit`, `-256colors`, `-64colors`, `-8colors`, `-8greycolors`, `-4greycolors`, `-2greycolors`

Set the color depth. Fewer colors can significantly reduce the required bandwidth.
Note: Grey colors only work with 32 bits color screen resolution. 16 or 24 bits color resolutions just don't work with grey colors.

`-shared`
Share the server with other viewers, i.e. allow several viewers to connect simultaneously to the server.

`-swapmouse`
Swap left and right button of the mouse.

`-nocursor`
Do not display any local dot mouse cursor.

`-dotcursor`
Display the local dot mouse cursor.

`-normalcursor`
Display the normal local mouse cursor.

`-belldeiconify`
???

`-emulate3`
Emulate a 3-button mouse.

`-noemulate3`
Do not emulate a 3-button mouse.

`-nocursorshape`
???

`-noremotecursor`
???

`-scale` *`A/B`*
Scale the display by the factor `A/B`.

`-emulate3timeout` *`Timeout`*
???

`-emulate3fuzz` *`Emul3Fuzz`*
???

`-disableclipboard`
Do not transfer clipboard content.

`-delay` *`delay`*
???

`-loglevel` *`loglevel`*
Set the loglevel. This can range from `0` (minimal) to `10` (maximum logging).

`-console`
Open a console window for log output.

`-logfile` *`filename`*
Log to the file specified by `filename`.

`-config` *`filename`*
Read the configuration from `filename`.

`-register`
???

`-encoding` *`encoding`*
Encoding is either `raw`, `rre`, `corre`, `hextile`, `zlib`, `zlibhex`, `tight` or `ultra`. Encodings are described here.

`-compresslevel` *`level`*
Use specified compression *level* (0..9) for "tight" and "zlib" encodings (Tight encoding specific). Level 1 uses minimum of CPU time and achieves weak compression ratios, while level 9 offers best compression but is slow in terms of CPU time consumption on the server side. Use high levels with very slow network connections, and low levels when working over high-speed LANs. It's not recommended to use compression level 0, reasonable choices start from the level 1.

`-quality` *`quality`*
Use the specified JPEG *quality* (0..9) for the "tight" encoding (Tight encoding specific). Quality level 0 denotes bad image quality but very impressive compression ratios, while level 9 offers very good

image quality at lower compression ratios. Note that the "tight" encoder uses JPEG to encode only those screen areas that look suitable for lossy compression, so quality level 0 does not always mean unacceptable image quality.

`-password` *`password`*

Use the specified `password` for "classic" VNC authentication.

`-serverscale` *`scale`*

Scale the display on the server side by `1/scale`. For instance `scale = 2` means that the remote screen dimensions are reduced by 2 ("half screen size"), reducing at the same time the amount of graphical data received by a factor 4 (2^2).

`-quickoption` *`option`*

Select a quickoption. Modem option is default.

- `1`: Auto
- `2`: LAN
- `3`: Medium
- `4`: Modem
- `5`: Slow
- `7`: Ultra

`-dsmplugin` *`filename`*

Use the DSM plugin specified by `filename`.

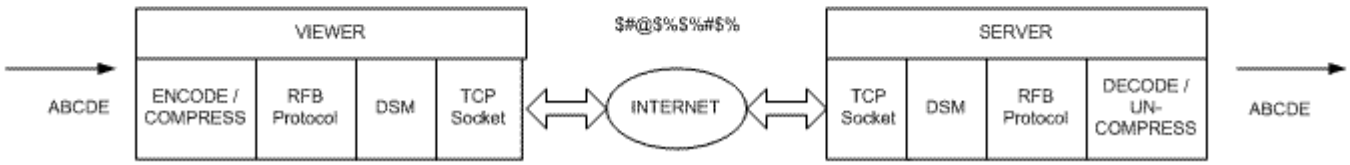
`-proxy` *`host[:port]`*

Use the repeater specified by `host` and optionally `port`.

9 MSRC4 Plugin Overview

9.1 DSM Overview

Ultr@VNC includes a basic Data Stream Modification plugin mechanism. It has been designed in the hope it is fast, efficient and minimizes the data and CPU overhead due to data transformation. It allows anyone to write an external dll that can be loaded by both Ultr@VNC Viewer and Utr@VNC Server. Then this dll has access to all the transmitted data packets and can consequently alter, modify, record, or encrypt the VNC data stream during the connections.
The DSM Plugin system is a "tunnel" for the VNC connection:



In the above example, the input "ABCDE" is encapsulated in the RFB protocol, and then sent out over the internet. Notice the text is still visible inside the RFB protocol packet. The server on the other end translates the text back to "ABCDE". In the DSM example, the text AND the RFB protocol wrapper are transformed by the plugin. The text and the RFB protocol wrapper are not visible on the internet. The server transforms the packet back to plain-text, then translates it back to "ABCDE".

9.2 The MSRC4 Plugin

The MSRC4 plugin uses the Microsoft Crypto API to encrypt the data stream using RC4 stream encryption This is the same encryption method used by SSL. RC4 encryption is secure but processor light, making it well suited to streaming data. The clear text and the encrypted text take up the same amount of space, making it simpler to code.
Unlike SSL, the keys are generated once, and then "pre-shared" onto the clients are servers that will use the encryption plugin. UltraVNC does not have a method for dynamically creating keys, and the DSM architecture was built in such a way that it is not possible for the plugin's to dynamically negotiate the keys.
The plugin is supported on Windows 95 through Windows 2003 Server. Key sizes supported are 40bit, 56bit, or 128bit. (The bit size is limited to 40bit on some versions of Windows. With the "High Encryption Pack" installed on 95osr2 or 98/98SE, they will support up to 128bit keys.)
The encryption method, key, and key length are stored in the key file generated by the plugin. Keeping your key files secure keeps your encryption secure. Changing your keys often is as prudent as changing your passwords often.
Currently there are two versions of the MSRC4 plugin. The first version stores it's configuration information in the Windows registry. The other version does not use the registry, but uses a combination of "default paths" and environment variables to locate the key file.
The "NoReg" version is msrc4plugin_noreg.dsm

9.3 ARC4 Plugin

ARC4Plugin - uses 128bit RC4 encryption. It does not require a pre-shared key. It adds a 128bit random SALT to your VNC password, then uses MD5 to create a 128bit hash, and uses that as the encryption key. This makes the key for each session UNIQUE. A random 128bit IV is added to the first block.

9.4 AESV2 Plugin

AESPlugin - V2 - 128bit AES encryption, OFB mode. It does not require a pre-shared key. It adds a 128bit random SALT to your VNC password, then uses MD5 to create a 128bit hash, and uses that as the encryption key. This makes the key for each session UNIQUE. A random 128bit IV is added to the first block.