


PIN Services UltraVNC Remote Control Use, Configuration and Administration


This document describes how to access the PIN Services Remote Control Service. It consists of two parts. The first part describes the normal configuration and use of Remote Control through UltraVNC. The second part describes how to configure the UltraVNC server and client to provide remote access.

Part A - Normal Configuration and Use



1. General Description of Remote Control

Remote control technologies have been around for a number of years but it has only been in the last several years that software and hardware has matured to the point that the technology has become easy to implement, reliable, and responsive enough to be generally usable. In a remote control connection the keyboard and mouse of a client machine is used to control the **Graphical User Interface** (GUI) of a remote PC, which is usually behind a firewall on a local network. The result is that the remote PC is being used as if one were sitting down in front of it, but by using another keyboard and mouse.

Server
 Remote controlling a PC requires two separate software components: a **server** and a **client**. These are simply the programs that facilitate the two points of contact – the computer to be controlled and the computer doing the controlling. The client is fairly limited in that its role is to connect to the remote PC, send the keyboard and mouse commands to the remote PC and provide a **Window** or **Viewer** displaying the **Desktop** of the remote PC. The server software is more complicated as it is the tool that authenticates and secures the connection as well as interpreting and carrying out the commands on the remote PC and sending the display information back to the client.

Client


Although remote control is very seamless there are some specific mental juggling acts and limitations that must be kept in mind and gotten used to when using remote control. These are:

-  Depending on the speed of your upstream and downstream connections there will be a lesser or greater lag time between sending a command and seeing a result. This may lead to, if one is not patient, a piling on of commands that leads to a dropped connection or crash. Much of the feedback provided by the operating system that lets you know something is happening - that your command has been initiated - is delayed via remote control. Patience is required when getting used to using remote control and performance will vary greatly from location to location, and depending on the time of day.
-  The greatest challenge is getting used to and keeping track of the fact that you now have two desktops, two taskbars, two Start Menus, etc. It will take some time, and practice in recognizing the cues that reliably determine whether any particular command you initiate is being sent to the PC you intend it to.
- When creating and moving around data it is also essential to be very clear about which machine, the client or the host, the data is created on and ends up on. This is particularly important in terms of ensuring that sensitive data is secured and backed up.
- Certain special key commands are not directly available as they will always be applied to the local PC. These are special **alt** and **ctrl** sequences that are generally not needed for normal

use such as **ctrl-alt-del** which brings up the **Task Manager**. These special commands may be accessed on the remote machine through an Ultra VNC Viewer menu if required.

The main use of remote control is to access a remote PC as if one were sitting in front of it. Since we are, in effect, using the PC as if we were in the office (and we are actually operating that PC indirectly) we also have access to all the network resources that PC does, including all the applications, data, network folders, printers, external drives, etc. In combination with the other services, FTP and VPN, remote control offers a different level of access that can supplement these other services based on specific need or loss of availability of these other services.

For example, if large or a large number of files need to be copied to the FTP share this can be accomplished more efficiently through remote control than through the VPN. If FTP is unavailable UltraVNC has a built-in FTP server/client feature that allows file uploads and downloads.





If the VPN is unavailable then email may be unavailable remotely. In this instance remote control allows email to be accessed through the office PC where the PST is actually stored.

Finally, remote control can facilitate trouble-shooting of these other services, computers, network devices, and the router since if a remote control connection can be established all the network resources can be 'indirectly-directly' accessed. With the 3 levels of service only imagination limits what is possible.

2. Configuration of UltraVNC Services on PIN03-newPC

The UltraVNC server software is installed on PIN03-OldPC in the office. It is configured for both secure and un-secure remote control. Normally in a remote control session there is no sensitive data being sent, only commands and connectivity information.

  The possibility does exist that a remote control session may be hijacked allowing a third party to facilitate their own access to the remote PC. For this reason, as with all other services, it is best to both secure and encrypt the sessions.

The first level of security is to require authentication to the server with a password. To secure the information that is being transferred it must be encrypted. There are several ways to do this. In this implementation if a secure (encrypted) remote connection is desired the **Virtual Private Network (VPN)** is used, which encrypts all data by default, **and is initiated before the remote control session**, and by using the IP address of the PC on the internal network or on the VPN rather than the router IP address. The router IP address is used for the unsecure (not encrypted) connection.



It is possible to use encryption built in to UltraVNC when remote controlling directly over the Internet but as the risks are relatively small and since if this is implemented the encryption has to be turned off when the VPN service is used (to improve performance) simply using the VPN for a secure remote control connection is more user-friendly. A description of how to configure the built-in encryption in UltraVNC is included in part B of this document in case it becomes preferable to using the VPN for securing remote control.



Using security certificates and encryption is an easy to implement, user-friendly, reliable, and extremely secure way of sending data through any service over the web. However, your security depends entirely on the management of certificates and passwords. If the certificates and passwords are not properly secured your system may be compromised directly.

Like all other services remote control is accessed through the IP address (and a port number) of the computer providing the service, and therefore, indirectly through the router connected directly to the Internet that the remote control server computer is behind. In the unencrypted case it is the IP address of the router that is used to access the actual remote control server. The internal network/VPN IP address is used for an encrypted connection. Most services are configured to use a domain name and DNS to be accessed. The PIN services remote control service is configured to be directly accessed through the **pin.dyndns.biz** domain.

Key Information for making a PIN Services Remote Control Connection



Server or Router IP address, or Domain: pin.dyndns.biz or <http://pin.dyndns.biz>
 Ports: VNC client port number is **XXXX** for both encrypted and unencrypted connections.
 Browser Java applet port number is **XXXX**. It is not encrypted in the current configuration.



User account for authentication: Windows Vista account on PIN03-newPC – **XXXXXXXXXX**
 Password: *********
 (stored in **XXXXXXXXXX** on PIN00-oldPC and on **XXXXXXXXXXXXXXXXXX**)

3. Connecting to the PIN Services UltraVNC server using UltraVNC client and Internet Browsers

A remote control connection to PIN03-newPC can be accomplished in several ways. Normally one uses the **UltraVNC client** (VNCViewer). This provides more tools for viewing and accessing the remote PC, as well as better graphics and response. Using an Internet Browser is very simple and only requires that Java is installed on the PC used to remote control. It is not as responsive and uses poorer graphics, but requires no client installation or configuration to use and is therefore useful in emergencies, for example when the laptop is unavailable.

a) Using UltraVNC client to remote control



Remote Secure

Pre-configured UltraVNC sessions have been created and placed on the desktop of **PIN02-newlaptop** to allow remote control of **PIN03-newPC**. There is a secure (encrypted) and unsecure (not encrypted) connection. The unsecure connection requires a password but is not encrypted. The secure connection is run through the VPN and will not work until the VPN is established. UltraVNC server on PIN03-newPC is configured to authenticate using a Windows account. The username and password of any local account will allow a remote connection to be made. The Windows account (username) to use is: **XXXXXXXXXX**

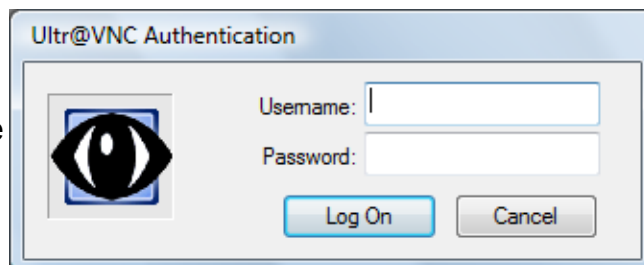


Remote Unsecure



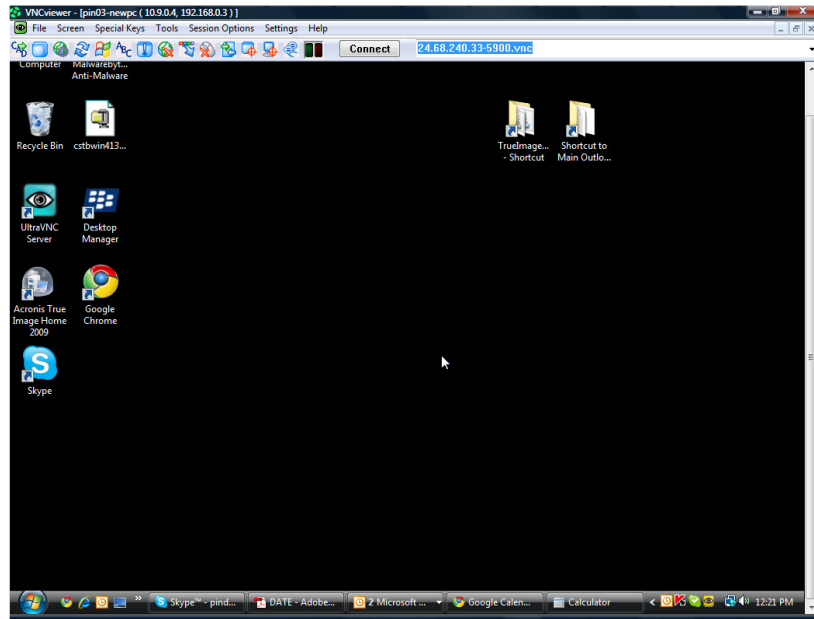
Both the remote control service and shared folders on PIN03-newPC are accessed through the local **Pin Services** Windows user account. For this reason the password for **Pin Services** needs to be carefully guarded to prevent compromising the system or data. It is a good practice to change this password every 6 months.

Doubling-clicking either icon will open the Viewer and the dialogue box shown to the right:



Enter the username **Pin Services** and the password and *click* **Log On**. The remote control

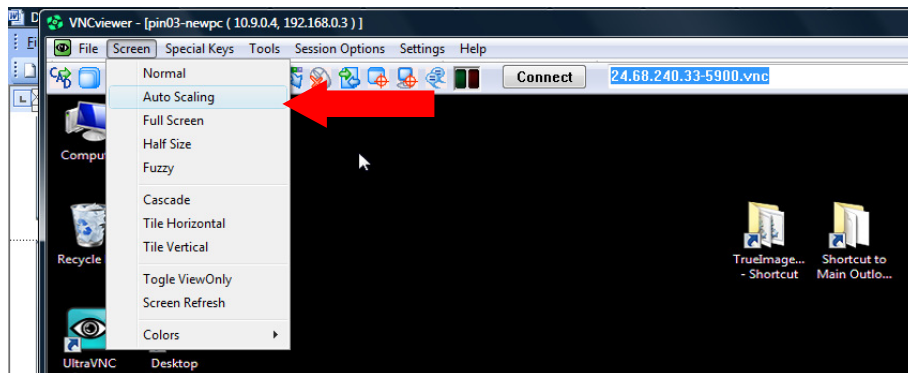
Windows, the **VNCviewer**, showing the desktop of the remote PC will open as shown below



The desktop wallpaper of the remote PC is not displayed in the remote control window to minimize the amount of data that is sent over the Internet. This improves response times.



One of the challenges of using remote control is keeping straight whether or not you are accessing the remote PC or the local PC. As the screen resolution of the 2 desktops is likely to be different the remote desktop is not likely to fit exactly into the monitor of the local PC. This means that you may have to scroll within the remote control window to see the entire remote desktop. There is a setting on the VNCviewer toolbar (shown below), **Screen | Auto Scaling**, that will rescale the remote desktop within the remote control window so that it fits exactly within the local monitor. Using this setting will distort the remote desktop slightly but makes it much easier to determine which computer you are actually interacting with at any given moment.



Once you have resized the remote desktop you can proceed to access the remote PC as if you were sitting in front of it.

To terminate a remote control session simply close the remote control window.

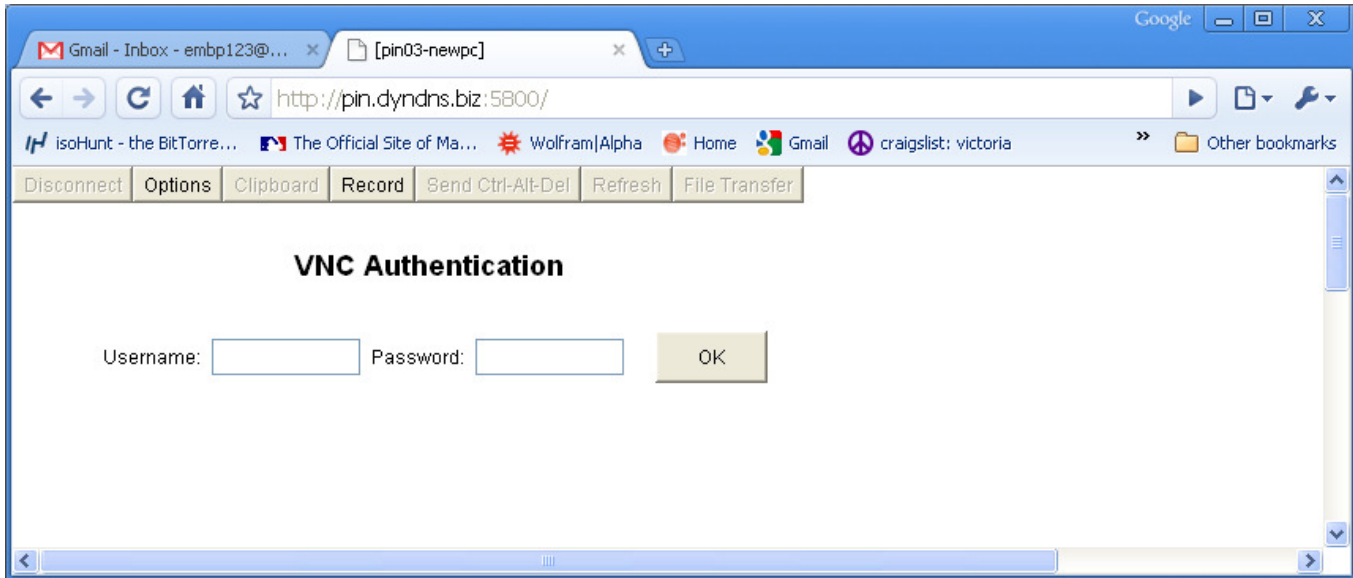
b) Using an Internet Browser to remote control

If the UltraVNC client is unavailable you may still remote control a PC using an Internet Browser.



Internet Browser remote control will only work if Java is installed and if the firewall is enabled for Port **XXXX** and IP address 192.168.0.3 (PIN03-newPC). See the document **PIN Services Network Config and Admin** for instructions on how to configure the router firewall for remote control using an Internet Browser.

To start a remote control session launch any Internet Browser. In the address field type the following information: <http://pin.dyndns.biz:XXXX> and *hit* **Enter**. The following page will open (Chrome is used in this example).

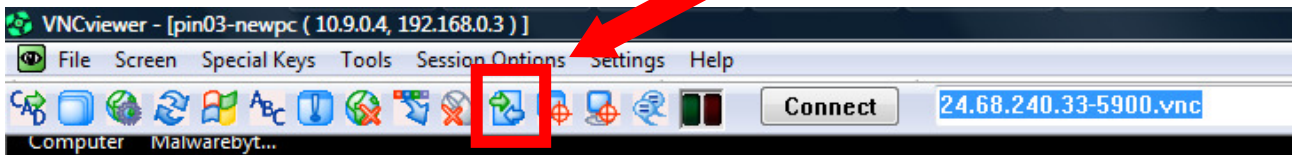


Enter the Windows account username **Pin Services** and the password and *click* **OK**. The remote desktop will now appear in the Browser and you may begin controlling the remote PC. To end the session either *click* the **Disconnect** button or close the page or browser.

c) Using the built-in File Transfer Capabilities of UltraVNC

Besides being able to remotely control a PC in the office you can transfer files to and from the server and client PC's using a built-in FTP server/client. This feature is available through both the UltraVNC client and when using an Internet Browser. When using an Internet Browser *click* the **File Transfer** button (see above).

When using the VNCviewer *click* on the **file transfer** icon on the VNCviewer toolbar

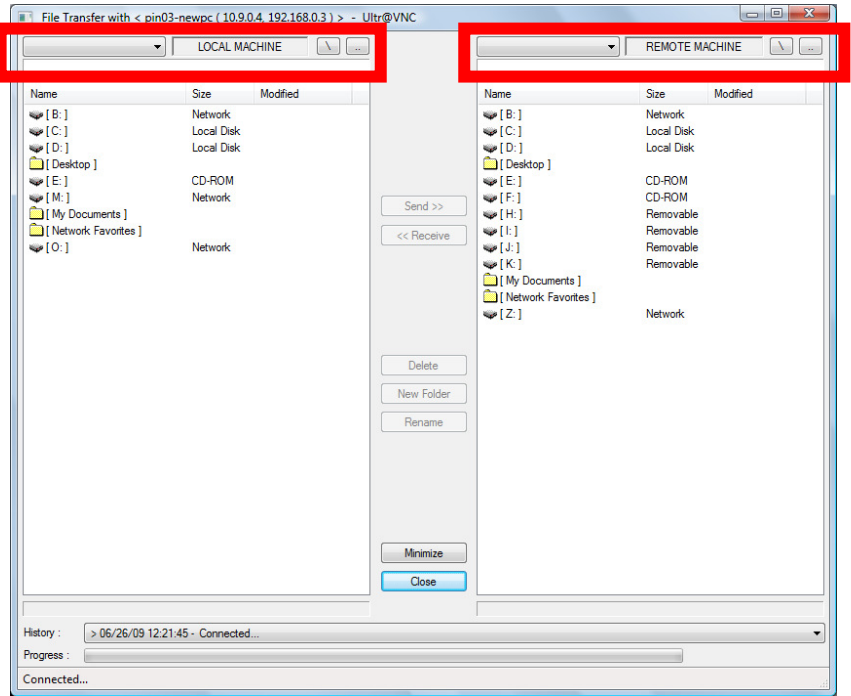


The following window will open:

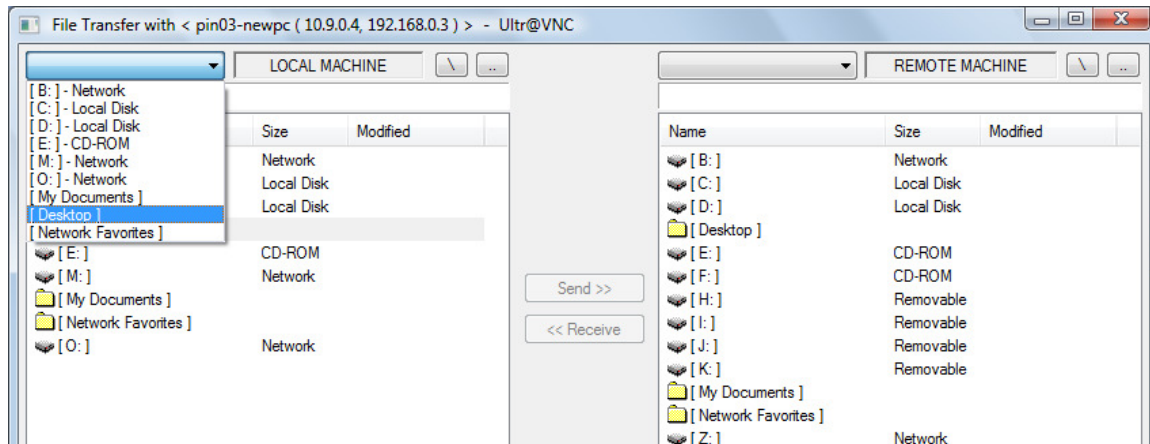
This is essentially an FTP client showing files and folder on the remote controlled (remote) PC on the right, and files and folders for the controlling PC (local) on the left.

The **drop-down menus** shown to the right allow you to select default folders on each PC. Use these menus and the **Browse Windows** below to browse for the files you wish to transfer and for the destination folder.

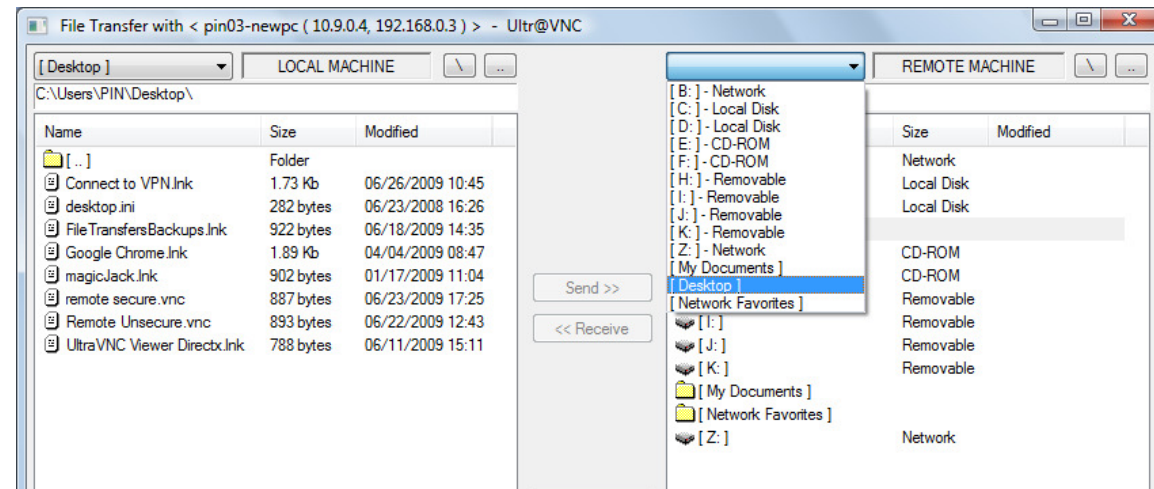
In the following example we will move a file from the desktop on the remote PC to the desktop of the local PC.



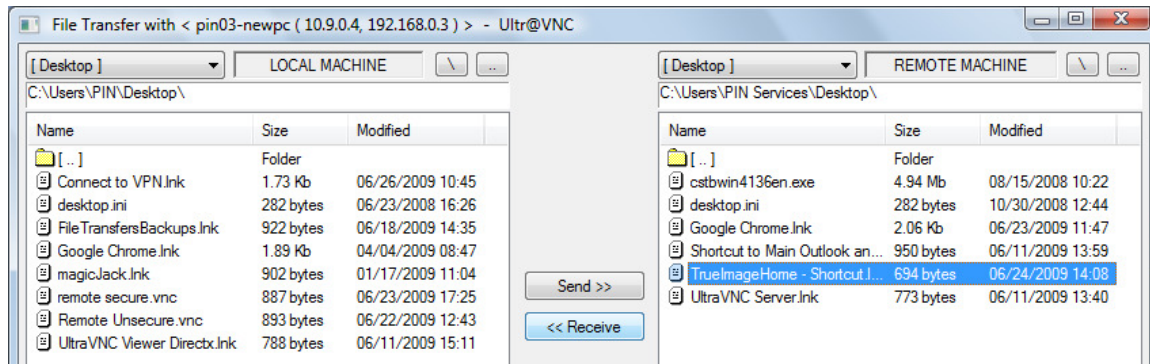
First **select** the Desktop of the local machine (shown below)



Next **select** the Desktop of the remote PC (shown below)



Now we will move the file **TruelmageHome – Shortcut...** by *selecting* the file and *clicking Receive*



Receive means download, and **Send** means upload.

When the transfer is complete simply close the File Transfer window.



You can not end a remote control session while file transfers are in progress or while the File Transfer window is open.

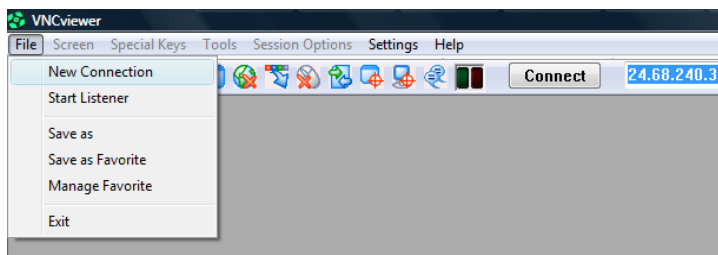
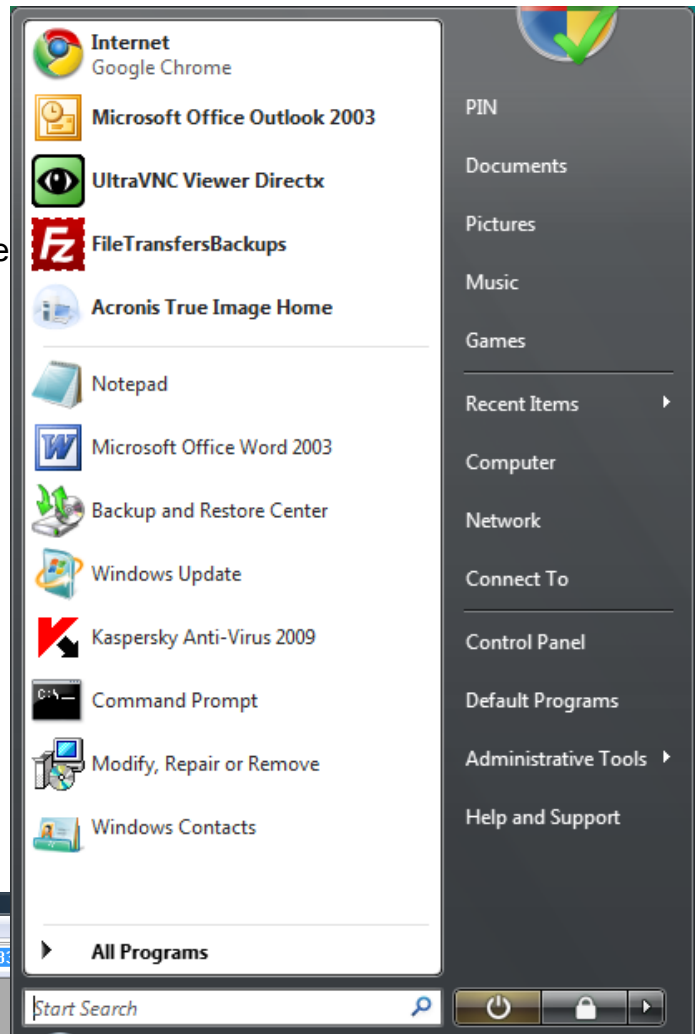
d) Initiating a remote control session manually.

If for some reason the pre-configured sessions do not work it is a simple matter to start a session manually. There are actually two versions of the UltraVNC Viewer, a basic and a DirectX version. The DirectX version offers better video performance and is the preferred version to run. The basic version is fine to use and might be helpful for troubleshooting. If the pre-configured sessions fail simply launch the UltraVNC DirectX viewer through the **Start Menu** as shown to the right or by *clicking* the **Start | All Programs | UltraVNC | UltraVNC Viewer DirectX**



Launching the DirectX version launches the entire viewer. Launching the basic version starts with the authentication dialogue box

Start the UltraVNC Viewer DirectX and then **Select File | New Connection** as shown below and the **Connection** dialogue box will open (shown on the following page)



To manually start a unencrypted remote control session type the following into the **VNC Server** field:

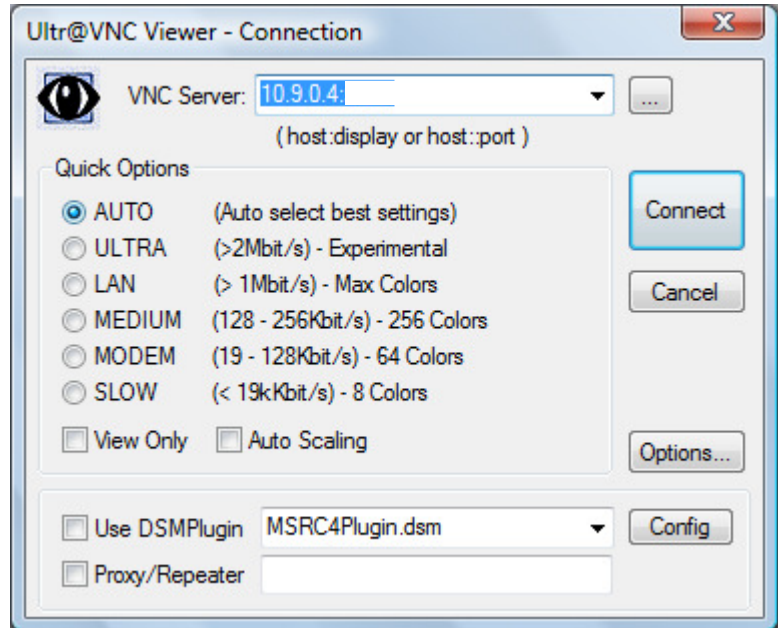
pin.dyddns.biz:XXXX

and *hit* **Connect**

For the secure encrypted connection start the **VPN** first, then this dialogue box, and type in:

192.168.0.3:XXXX (not as shown)

and *hit* **Connect**



You will now be prompted to provide a username and password as usual.



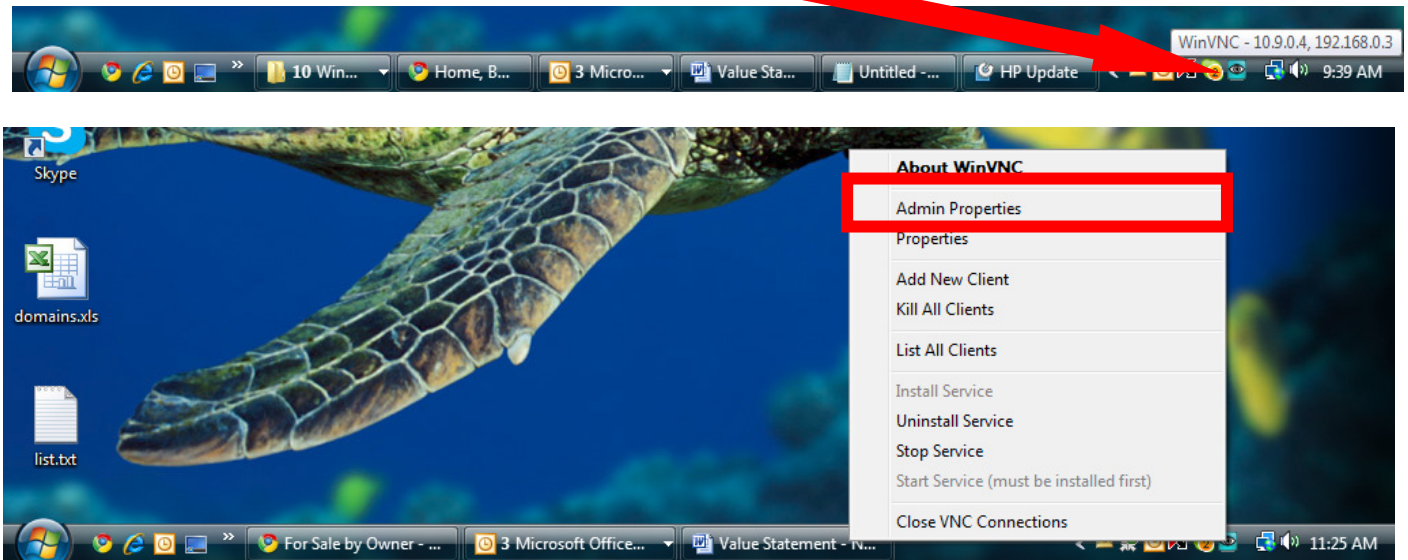
Notice the **Use DSMPlugin** checkbox. If you *check* this box when using the unencrypted connection over the Internet this will enable UltraVNC's built-in encryption for that session. To enable UltraVNC's encryption on the server see Part B of this document. When using the VPN this additional encryption is not needed and would slow down response.

Part B – Administration and Configuration of UltraVNC

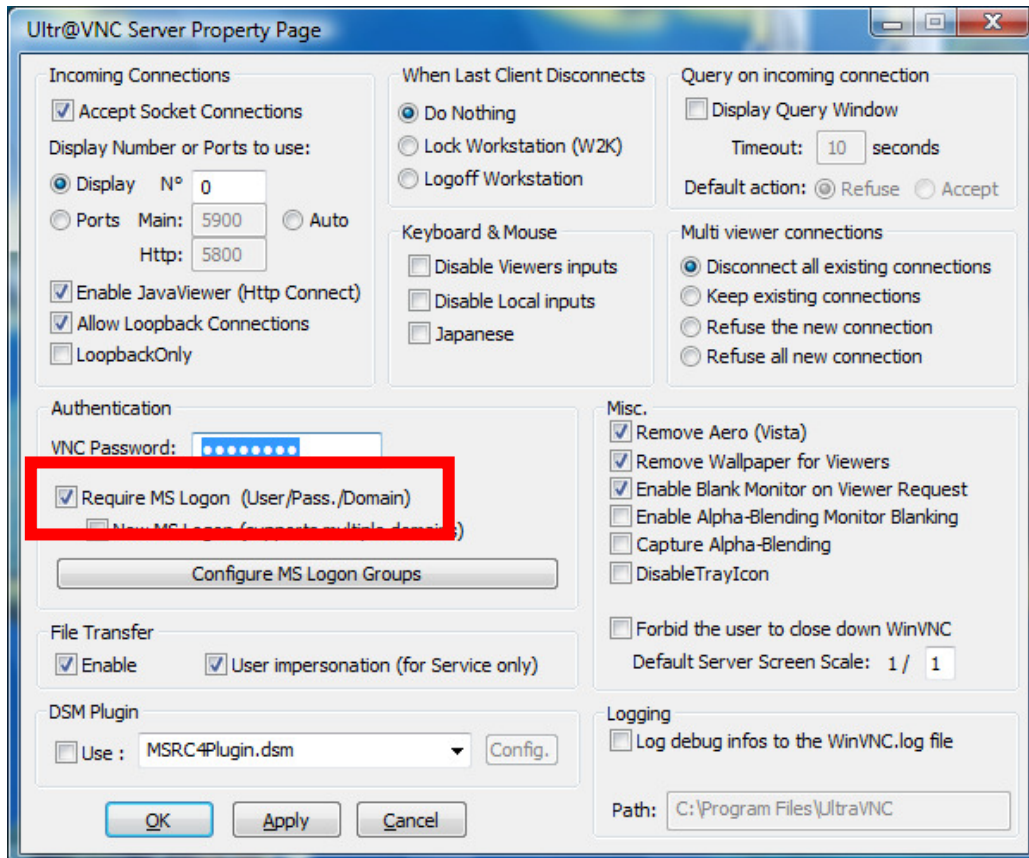
This part of the document provides additional configuration information for trouble-shooting.

1. Configuration of UltraVNC Server

UltraVNC Server is installed and configured on PIN03-newPC. The configuration is very simple and snapshots are included here for trouble-shooting. The UltraVNC server can be administered by *right-clicking* on the icon tray UltraVNC server icon and *selecting Admin Properties*



The key configuration change made is to enable the **Require MS logon** feature by *checking* the checkbox shown below:



All other settings are default settings.



PIN00-newPC has been configured with a static IP address on both the local network and the VPN. Static IP addresses facilitate routing through the firewall.

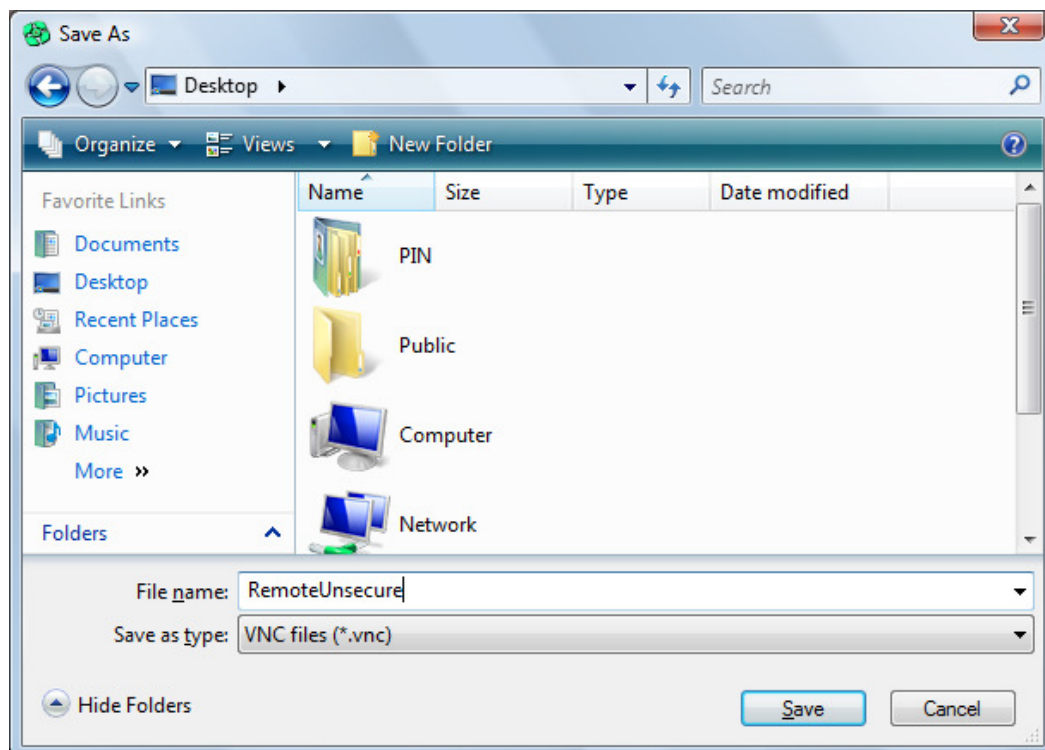
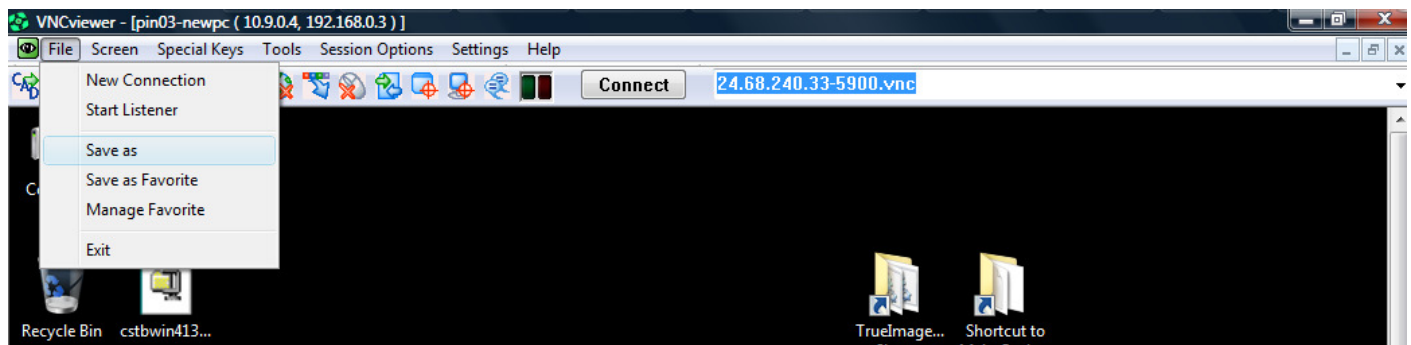
The IP address of PIN03-newPC on the local network is 192.168.0.3 (Port **XXXX**, and **XXXX** are forwarded through the router to this IP address).

The IP address of PIN03-newPC on the VPN is also 192.168.0.3 (use this IP address through the VPN for an encrypted remote control connection).

If the **Use** checkbox is *checked* for the **Use DSMPlugin** then the built-in encryption will be enabled by default on all sessions.

2. Configuring new session icons

If the pre-configured sessions fail it is a simple matter to make new ones. Delete the non-functional icons and start a manual remote control session. Once the session is established **select File | Save as** and *browse* to the Desktop and *save* the session with an appropriate name, either RemoteSecure or RemoteUnsecure, as shown in the two snapshots below.

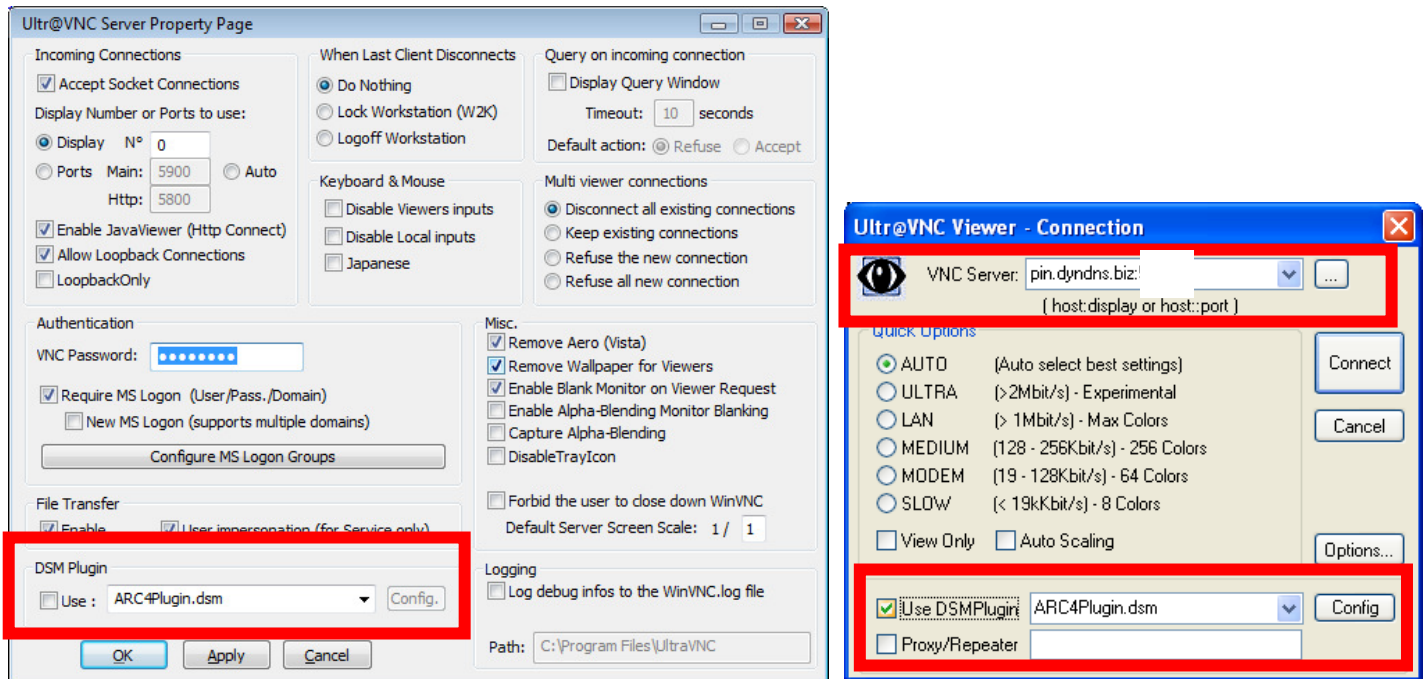


3. Implementing UltraVNC's Built-in Encryption for a Remote Control Session

If for some reason you need to improve the security for a remote control session but can not use UltraVNC through the VPN, which encrypts all PIN Services network communications when initiated, you can enable the built-in encryption.



An encryption plugin, **ARC4Plugin.dsm**, and key, **arc4.key**, have been installed on all PIN Services PC's. To implement the use of this encryption plugin and key you must access the UltraVNC administration panel on PIN03-newPC as described earlier in this document, and shown below.



Simply *check* the **Use** checkbox for the **DSM Plugin** setting in the lower right of the admin window and *click* **OK**.

It may be necessary to *Stop* and *Restart* the UltraVNC Server to enable encryption. This seems to be a bug in the software. The general procedure for stopping and starting (restarting) a **Windows Service** may be found in Part B of the document, **PIN Services OpenVPN Configuration.doc**

Once the UltraVNC admin panel has been reconfigured and the service restarted simply *double-click* the **Unsecure UltraVNC** session icon or follow the instructions for a manual connection.



If you use the pre-configured icon to connect you will first receive an error dialogue box informing you that you need to select the encryption plugin. Simply *click* **OK** to continue.

When the authentication windows appears (shown above right) enter the information as shown or *select* the information from the **VNC Server** field drop-down menu, *check* the **Use DSMPlugin** checkbox and then log in as you normally would.

To disable the encryption simply repeat these steps but *uncheck* the appropriate boxes on the server and client.