FUTUREDESIGN CONTROLS

Orion *nCompass* i4.3 VNC Networking Guide

Orion nCompass i4.3 VNC Networking Guide Rev B
August 2014
Supersedes: Rev A (June 2013)

1 Smart Networking Practices

The expansion of Ethernet onto the industrial floor has brought forth a new realm of possibilities from the gathering of information to the inherent control of equipment from anywhere around the world. The flexibility and convenience that this provides makes it a very desirable feature for new equipment. nCompass provides this ability, but there are considerations that must be taken by the end user to protect their equipment and investment.

Just like placing a personal computer on the internet opens it up to outside attack, placing your nCompass on a network poses the same risk. The first thing to remember is this: The most likely cause of problems is not a hacker trying to sabotage your equipment, but more often to be related to the ubiquity of PCs with Ethernet cards, the ease with which your own co-workers can 'hang stuff on the network,' and careless or nonexistent internal security measures. Accidental problems are more common than deliberate ones.

Allowing anyone access to nCompass by placing it on the office LAN, also opens the door for accidental shutdown, damage to equipment, loss of data, lost time, etc. This is possible even by the most well-intentioned co-workers. Thus, there are several steps that should be taken to minimize this risk.

The first is to never mix your office LAN with your control LAN. The control LAN should be a separate network that consists of your nCompass controller(s) and possibly any other equipment that you may have that is related to the operation of the system. It should be separated from your office LAN by a firewall, or at minimum, a bridge or router. A control network and a business network have two entirely different purposes and their interaction should be closely controlled.

It is also unwise to assume that any Ethernet capable devices themselves have any security features at all. The nCompass VNC server only provides minimal single-password based security access. Separating the control LAN from the office LAN using a firewall would increase security and only allow control access that is based on a combination of IP source address, destination address, and port number. This is by no means completely 'hacker-proof,' but it should keep the well-meaning co-workers out.

Another hazard is connecting consumer 'plug and play' devices to your control LAN. A printer for example, might flood the network with traffic in a 'broadcast storm' as it tries to self-configure or advertise its presence to all nodes on the network. Faulty devices, for example defective NIC cards, can transmit large amounts of bad packets (i.e., runts, which are abnormally short Ethernet frames) into your network. Using switches instead of hubs will limit the effect of such problems.

The most commonly overlooked source of problems is cabling. Not all cables are created equal. Electrical noise generated by factory equipment or other electrical equipment in the area, could easily corrupt transmitted data over the network and cause devices to 'lock up' or shut down the VNC server, both of which then require nCompass to be shut down and restarted to clear the problem.

Select the right cable for the environment. Shielded twisted pair (STP) cable is naturally more noise immune and is preferable to unshielded twisted pair or UTP in noisy situations. STP should have at least 40dB CMRR and less than 0.1pF capacitance unbalance per foot. Ground STP cable, making sure the ground is connected only at one end. CAT5 STP patch panels normally provide a grounding strip or bar. Hubs and switches don't provide grounding, use cables.

It's wise to be pessimistic about a cable's ability to reject noise from 230 VAC and 460 VAC power lines and electrically 'noisy' equipment in the area. Capacitance imbalance in cables greater than 70pF per 100m can introduce harmonic distortion, resulting in bit errors. The cost of cable is quite small compared to total equipment cost, so if you're looking to save money, this is not a place to do it. Choose a well designed cable to minimize bit-error rate after installation, and that will give faster throughput with fewer glitches.

2 Configuring the nCompass Network

In order to connect to the VNC server of nCompass, you will need to know the IP address of nCompass on the network. It is important to note that if using DHCP in your network router, the nCompass address may change on re-power requiring you to access the nCompass controller directly in order to obtain the new IP address. This could result in VNC connection issues if the address regularly changes.

Therefore, it is recommended that the IP address for nCompass be assigned as a fixed (static) address. This insures that the address will not change once it has been set. This can be done in one of two ways. The first is by setting up the control LAN router to assign the same IP address whenever it detects the nCompass device on the network via its own identifier; it's MAC address.

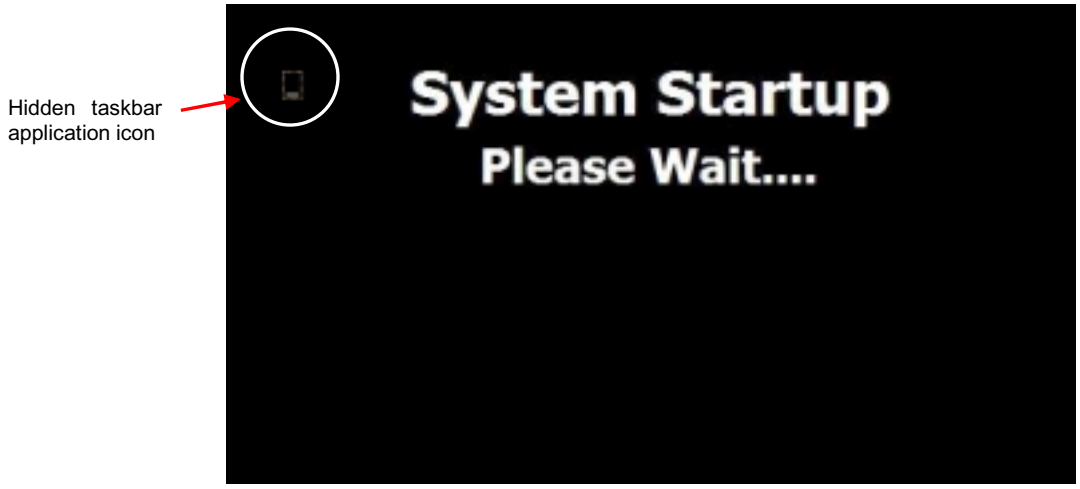
The other option is to configure nCompass to use a fixed IP address and disable the DHCP addressing function of its network interface. When using this method, it is important to make sure that the address being assigned to nCompass is not used by any other device on the network. If another device is using the same address, the VNC interface will not function correctly. It is recommended that this method of static IP assignment be used as it removes the IP address lease renewal process that would be performed by the control LAN router if DHCP was used.

The lease renewal process performed by the control LAN router can cause the VNC server in nCompass to shut down due to an issue in the renewal process. It could be caused by something in the router firmware or configuration of the router itself. Due to the numerous brands and models of routers available, and the dynamic nature of their use, attempting to resolve the issue is beyond the scope of this guide. Therefore, the use of static IP addressing removes this from the equation, providing the most robust network solution.

2.1 Obtaining the nCompass MAC Address

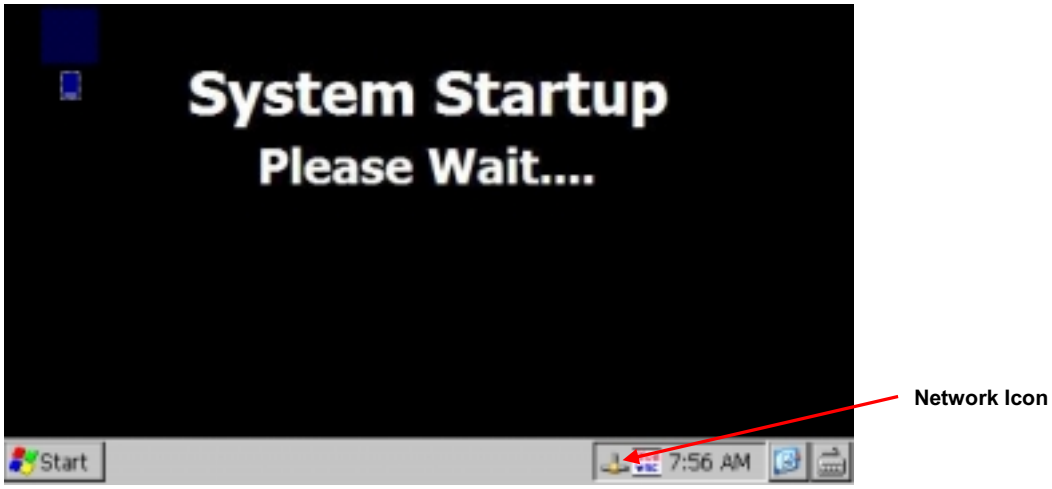
The MAC address can be obtained from the network connections screen. In order to access the screen, you must exit the nCompass application. To do so, proceed to the 'Exit Application' screen under the offline setup menu. Press the 'Exit and start runtime on next power up' button to exit the nCompass runtime application. Follow the on screen prompts to stop the application and exit to the Windows CE desktop.

NOTE: The text, "System Startup Please Wait…" on the desktop is static and does not indicate that any application is going to start at this time. It is used as a "placeholder" prior to the nCompass runtime or configuration application starting during normal power-up sequences so that the user is informed that an action is taking place.

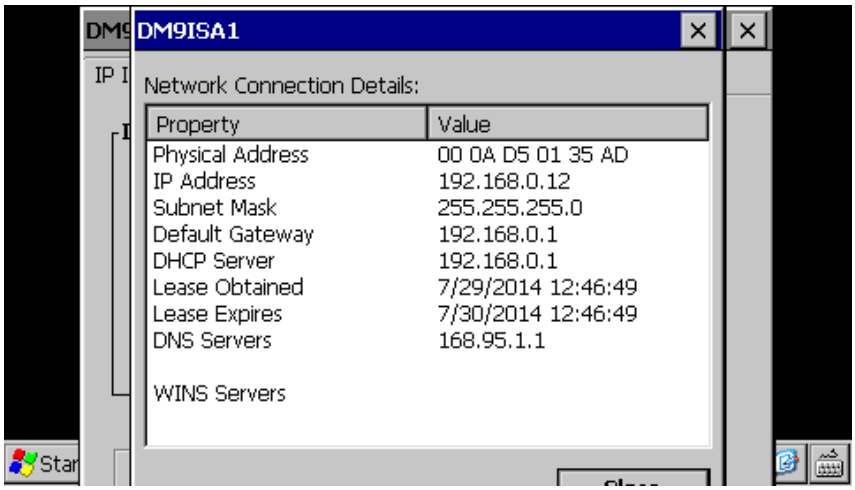


From the desktop, double-tap the hidden icon at the top left of the screen to provide access to the taskbar application.

Press the 'Show Taskbar' button in order to show the taskbar and then press the 'Quit' button to exit the taskbar application.



Next, double-tap on the network connections icon to open the network connection information window. Two tabs will be provided; one for IP Information and the other for IPv6 Information. To obtain the MAC address, press the 'Details…' button on the IP information tab.



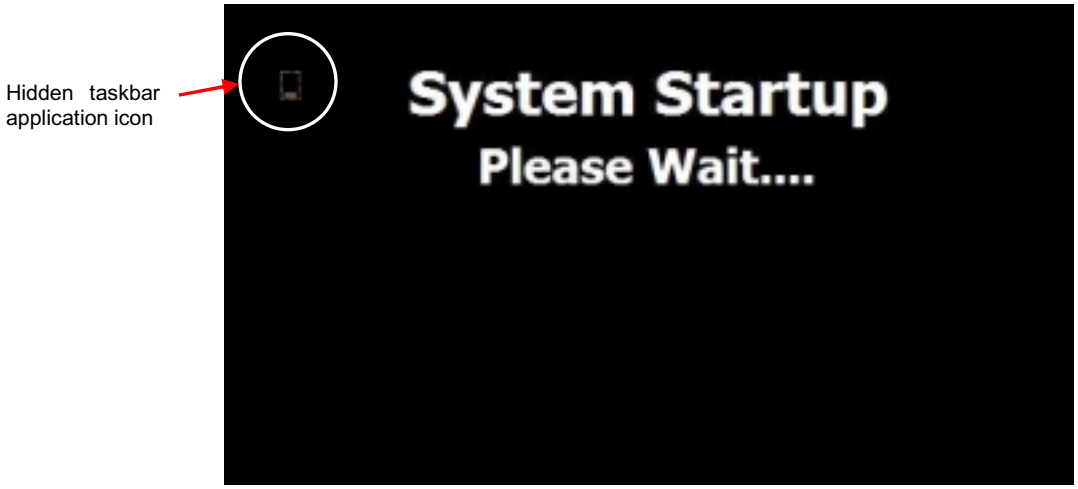
The MAC address is displayed as the first item (Physical Address). Once the address has been recorded, close the network information windows and cycle power to nCompass in order to restart the system and return to normal operation.
return to normal operation.

2.2 Setting nCompass to a Static IP Address

In order to set a static IP address for nCompass on a network, it requires you to exit the nCompass application and enter the 'Network and Dial-up Connections' settings of the CE operating system.

IMPORTANT: ***It is recommended that only personnel charged with configuring and maintaining nCompass perform this procedure. Do not alter, change or delete any other files or settings of the system. Doing so may render nCompass inoperable.***

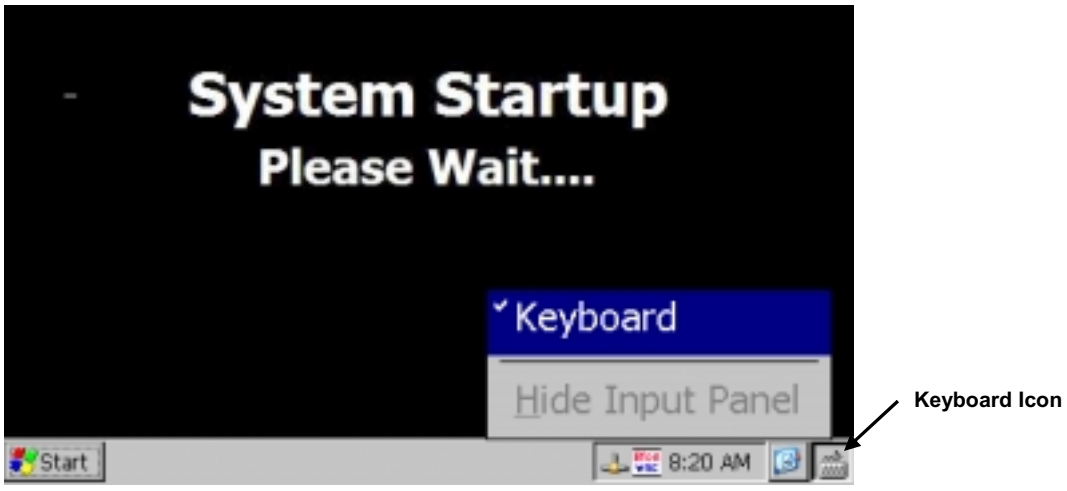
To begin, you must exit the nCompass application. To do so, proceed to the 'Exit Application' screen under the offline setup menu. Press the 'Exit and start runtime on next power up' button to exit the nCompass runtime application. Follow the on screen prompts to stop the application and exit to the Windows CE desktop.



NOTE: The text, "System Startup Please Wait…" on the desktop is static and does not indicate that any application is going to start at this time. It is used as a "placeholder" prior to the nCompass runtime or configuration application starting during normal power-up sequences so that the user is informed that an action is taking place.

From the desktop, double-tap the hidden icon at the top left of the screen to provide access to the taskbar application.

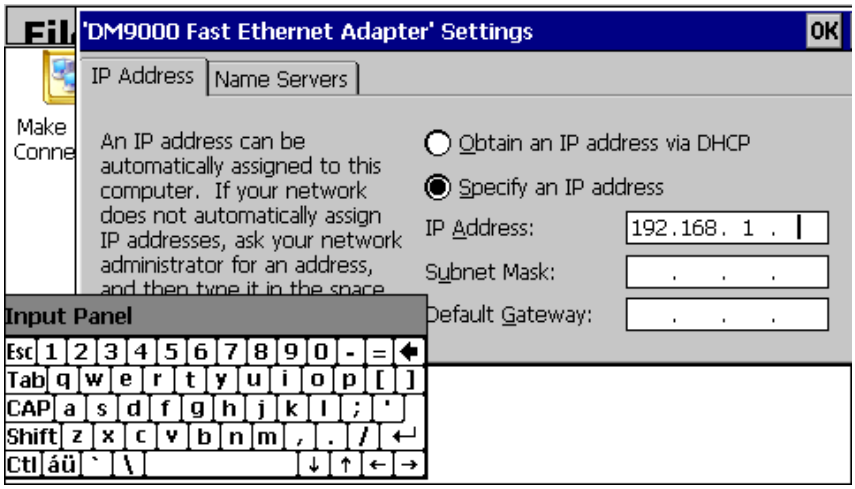
Press the 'Show Taskbar' button in order to show the taskbar and then press the 'Quit' button to exit the taskbar application. Before proceeding any further, enable the CE keyboard so that it will be available to enter in the IP address. If you do not enable it now, you will not be able to access the taskbar later once in the Ethernet Drivers screen.



To enable the keyboard, touch the keyboard icon at the lower right of the taskbar and select 'Keyboard' from the menu. This will make the keypad visible. Next, press the Windows Start button and select 'Settings' and then 'Network and Dial-up Connections' to show the connections window.

From the 'Connection' window, select the current network connection by 'double-tapping' the connection icon to enter its property window. DO NOT create a new connection. The 'Ethernet Drivers' property window will allow you to set the IP address as well as name primary and secondary DNS and WINS servers from the 'Name Servers' tab if necessary. Select 'Specify an IP address' and enter in the desired IP address, subnet mask and default gateway.

You can move the keyboard around on the screen to position it as necessary to access the different fields. Once complete, close the 'Ethernet Drivers' window by pressing the 'OK' button located at the top right of the window. Next, close the Connection window by pressing the 'X' button at the top right of the window.

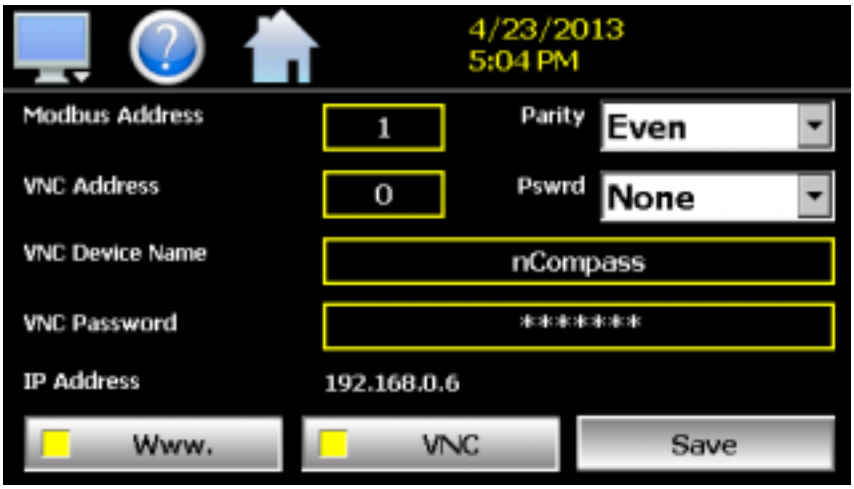


Access the taskbar and hide the keyboard by pressing the keyboard button at the bottom right of the taskbar and select 'Hide Input Panel'. DO NOT cycle power to nCompass at this time. Wait approximately 2 minutes before removing power. This provides time to allow the Windows CE operating system to save the new network settings to the registry so that it uses the settings on the next reboot.

If power is cycled too soon, the network settings will revert back to the previous settings on the next power up. Once the 2 minute time period has elapsed since updating the network settings, cycle power to nCompass in order to restart the system and return to normal operation with the new network settings.

2.3 Configuring the VNC Server in nCompass

In order to access nCompass via VNC over its network connection, the VNC server must first be enabled. By default, the server is disabled with no password required and an address of 0. Before using the VNC server, it is recommended that the default settings be changed to better suite your specific installation.



The VNC address and password set access rights to the nCompass VNC server. Valid addresses are from 0 to 255. However, it is recommended that the default address (0) not be used. An nCompass specific address in the range of 1-255 should be used to identify each nCompass device on the network. The default address of zero instructs the server to respond to any VNC client query with an unspecified port number. This can cause the server to see other unrelated network traffic, possibly causing it to shut down which requires nCompass to be restarted in order to restart the server.

IMPORTANT: *When multiple nCompass controllers are connected to a single router, it is imperative that each nCompass have a different VNC address. If multiple nCompass controllers have the same VNC address, network errors may result causing the VNC server to shut down or cause nCompass to "lock-up" and become non-responsive requiring the unit to be power cycled in order to return to normal operation.*

The VNC password selection defines the connection mode for the server. The selections are "None" and "VncAuth" which requires users to enter the password when connecting to nCompass over the VNC interface. It is recommended that you enter a new password and enable the password protection to minimize the chance that unauthorized people can gain access to nCompass.

The VNC device name field is used to enter a name (up to 35 characters) that can better identify nCompass to users logged into the VNC interface. The name entered here will be used on the VNC header window on a PC, so that if multiple VNC clients are open to different systems, each one can be identified. It is recommended that the default name be changed on networks with more than one nCompass device so that users are not accidentally operating the wrong unit.

Once all the proper settings have been entered, press the VNC button at the bottom center of the screen to enable (or disable) the VNC server and press the 'Save' button. This will save the new settings so that they will be used on the next power up. Cycle power to nCompass in order to complete the setup. If power is not cycled, the VNC server will not operate or will still be in operation under the previous settings.

3 Using the VNC Server

The nCompass VNC server allows a user to remotely monitor and control nCompass by directly viewing and manipulating the touch screen over the network. You must use the assigned IP address and VNC port number to access nCompass. The IP address is listed as the 'Device IP Address' shown on the communications screen. Write down the IP address and port number so you will have it to enter into your VNC viewer.

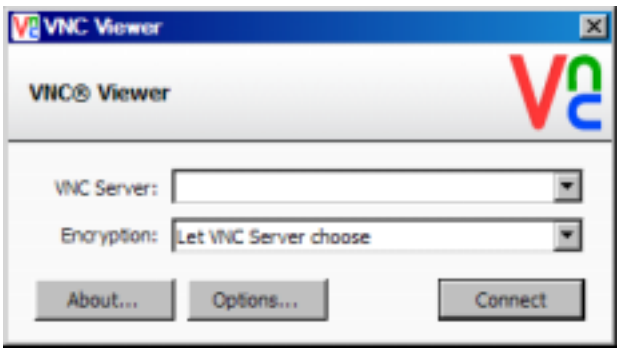
There are many VNC viewers available for both PC and tablet use. Due to the ever changing market and availability of such applications, it is not possible to test them all for compatibility or provide assistance for their use with nCompass. It is the responsibility of the end user to test the chosen VNC client for compatibility with nCompass prior to putting the unit into service. If the VNC client viewer has compatibility issues with nCompass, it can cause the VNC server to stop responding and/or shut down requiring power to be cycled to nCompass in order to reboot the system and restart the server.

Future Design Controls has tested and recommends the use of RealVNC's viewer. It has been tested for compatibility with nCompass and a free version can be obtained from http://www.realvnc.com/ for PC/MAC use. RealVNC does offer a version for the iPad that can be obtained through the App Store for a small fee. The App Store also offers a free VNC client called Remotix for the iPad. It has also been tested for compatibility with nCompass.

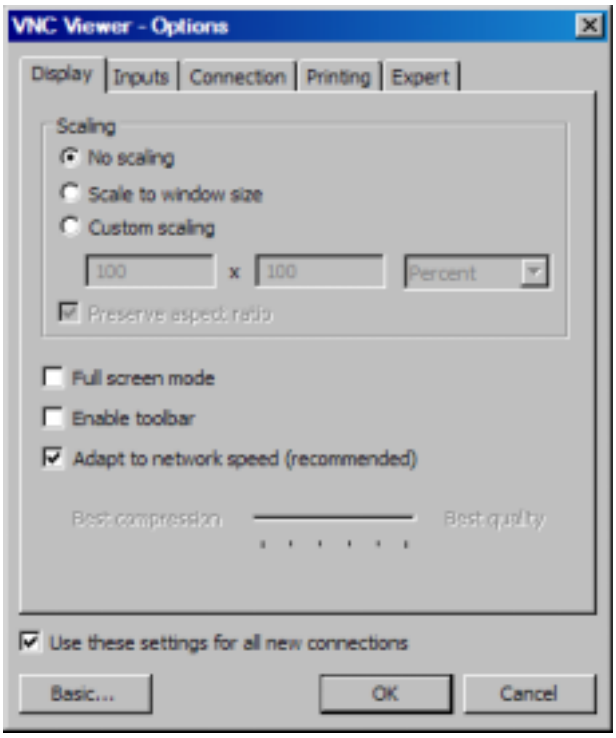
3.1 Recommended VNC Viewer Settings

This section applies to setup of the recommended RealVNC viewer for PC/MAC. These settings have been tested and evaluated in order to provide the best performance and quickest response to user input when using the VNC viewer with nCompass. After installing the VNC viewer software, it is recommended that the following changes be made to the default viewer settings.

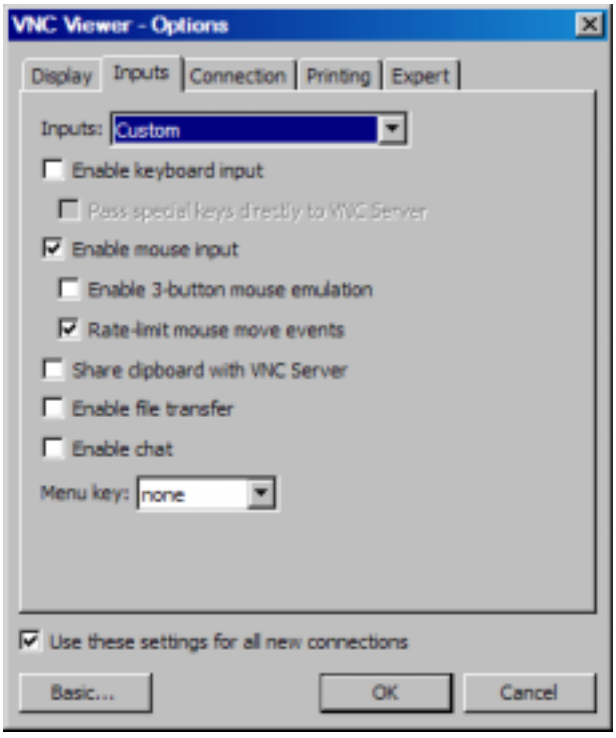
To begin, start the VNC viewer. Click on the 'Options' button in order to open the 'VNC Viewer - Options' window.



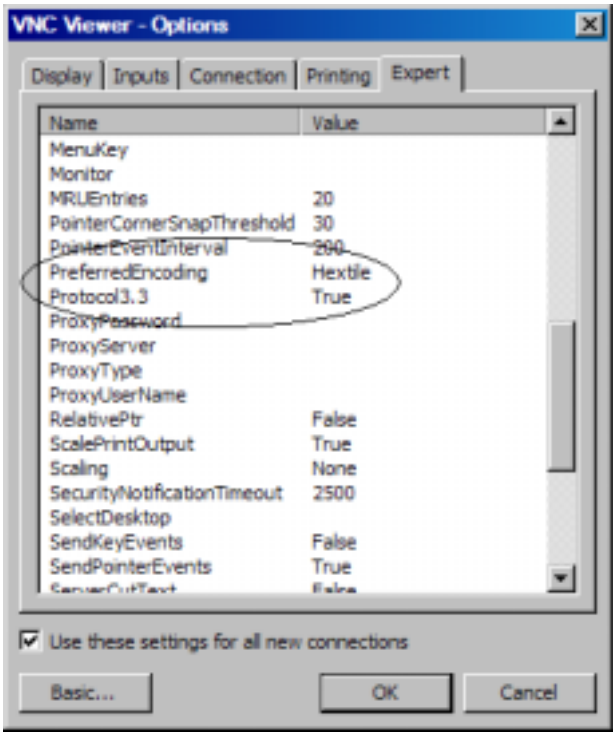
Click on the 'Advanced' button at the bottom left of the window in order to show the advanced setup options. On the 'Display' tab, make sure the scaling is set to 'No scaling' and the checkbox for 'Adapt to network speed (recommended)' is checked.



Next, select the 'Inputs' tab and deselect all entries except for 'Enable mouse input' and 'Rate-limit mouse move events'. The 'Inputs:' drop down selection box will automatically change to 'Custom' when the settings are made.



Proceed to the 'Expert' tab. Scroll down the list of settings until you find the 'PreferredEncoding' and 'Protocol3.3' options. Set the preferred encoding to Hextile and the Protocol 3.3 option to true. Verify that the 'Use these settings for all new connections' checkbox at the bottom of the window is checked and click the OK button. This will set the selections to the default start settings for the VNC viewer.



3.1.1 VNC Viewer Settings for Tablets

The VNC clients for tablets have been found to offer limited flexibility for use with nCompass. Most clients have default settings requiring security to be enabled on the server in order to connect. If you have trouble connecting with a VNC viewer through an iPad, iPhone or even an Android based phone, start by enabling the security on the nCompass VNC server and be sure to enter those settings in the client viewer.

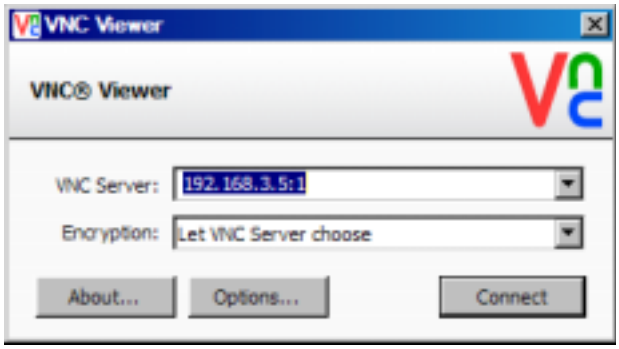
Color and encoding options can also affect the connectivity. If the client offers the option, leave color and encoding options to 'automatically detect' or 'server decides'. If the client is still unable to connect, try defaulting the encoding to Hextile and the color option to limited colors such as 256 bit color. FDC does not write or create VNC clients (3rd party software), so final selection of client and testing is the end user responsibility. The following settings are provided as an example for the Remotix client for the iPad. When adding an nCompass server to the Remotix client, use the following settings. Note that the VNC server in nCompass must have security enabled in order for this client to connect.

Connection Type:	VNC
Host/IP:	*IP address of nCompass*
Port:	*VNC address of nCompass (5900 = 0, 5901 = 1, etc…)*
Use SSH Tunnel:	Off
VNC Authentication:	VNC Password
VNC Password:	*VNC password of nCompass*
VNC Server Type:	AutoDetect
Operating System:	Windows
Preferred Encodings:	Hextile
Color Depth:	16 bits

3.2 Accessing nCompass through a VNC Viewer

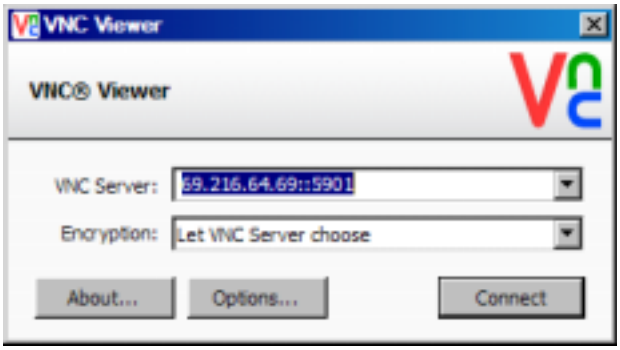
The following examples are based on the use of the RealVNC viewer for PC/MAC. Once the default settings have been entered, just enter the IP address and port number for nCompass, and click the 'Connect' button to access nCompass over the network.

Intranet Example: If the IP address assigned is 192.168.3.5 and the configured VNC Address is 1, from the PC's VNC Viewer address field, enter '192.168.3.5:1' to access the device (address 1 relates to port 5901, address 2 to port 5902, etc., which is the port opened by the VNC interface in order to allow communications with nCompass over the network).



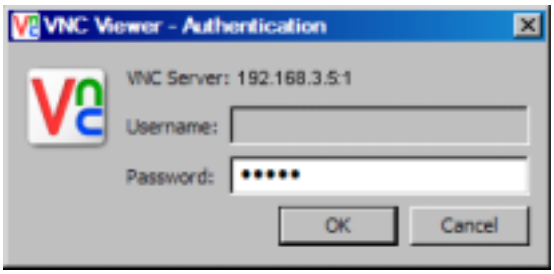
Internet Example: Internet connection typically requires a qualified network System Administrator. Typically a permanent IP address and specific port address are assigned to nCompass; support on this action is beyond the scope of this guide. *Consult your network system administrator for assistance in setting up an Internet connection.*

If the IP address of the LAN is 69.216.64.69 and the configured VNC Address is 1 (port 5901 has been opened and assigned to this specific nCompass controller), from the remote PC (outside of the site Servers LAN), in the VNC Viewer address field enter '69.216.64.69::5901' to access the device (5901 relates to address 1, 5902 to address 2, 5903 to address 3, etc., note the double colon).

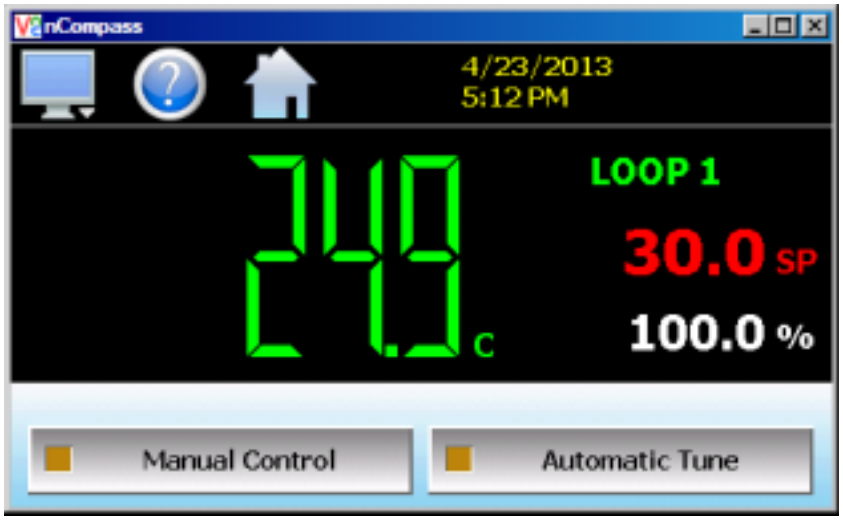


NOTE: The IP address shown on the communications screen of nCompass is the LAN address and would not typically be used for an Internet connection.

Security Example: If the VNC server password is enabled on nCompass, for either example above, upon pressing the 'Connect' button to make the connection, the VNC viewer will prompt for the proper password. The connection will only be established once the valid password is entered.



Once the connection is established, the current nCompass display will be shown on your desktop. The image will be a duplicate of what is on the nCompass. As you manipulate the screen, the display of nCompass will also be manipulated so that any local operator will be able to see what is happening and vice versa.



Multiple instances of the VNC viewer can be started on your PC. By running multiple viewers, you can have access to multiple nCompass controllers right from your desktop. The heading of each VNC viewer window will use the 'VNC Device Name' entry for the header. By entering a unique name for each nCompass, you can identify each VNC connection and know which system you are accessing.

The VNC viewer is meant to be used for short term control access to nCompass. It is not meant for long term monitoring of system operation. If long term monitoring access is desired, use the built-in web server of nCompass or a PC with FDC software to monitor and control nCompass over its serial communications port. The web server interface and PC software is designed for long term monitoring and status updates.

Due to the nature of VNC operation, and for security reasons, the VNC viewer connection should not be left open on your desktop. The viewer connection should be opened in order to perform the necessary control and/or status check of system operation, and then closed once the task is complete. Accidental manipulation of the control or erroneous network activity could cause connection problems over the VNC interface and result in the VNC server shutting down and requiring nCompass to be restarted in order to regain access.

NOTE: *Some viewers may also contain additional features for file transfer and other high level functions. These functions are NOT compatible with nCompass. Any attempt to use them may cause the nCompass VNC server to malfunction and require power to be cycled in order to reboot the system. All viewers should be used ONLY to monitor and manipulate nCompass as if you were standing directly in front of it.*