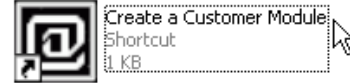


## — Quick Start Guide —

1. Run the Advantig-OneClick-Setup.exe program to install the viewer and creator programs and add icons to your desktop. The setup program will give you the private IP address of your workstation. Write down the address, you may need it when you open the port(s) in your router.
2. You must open the firewall or NAT router ports you plan to use for your customer modules to allow incoming traffic and direct it to the proper computer. For now lets use port **6080** to get familiar with the process. Visit the website for the manufacturer of your device or try **<http://www.PortForward.com>** for step-by-step instructions on many popular devices.

3. Run the “Create a Customer Module” program to create the Listen icon you will need to test your port. This also creates the customer module you distribute to your remote customer. For now use the examples below to ensure your port is forwarding through properly. You can choose other options later when you build your real customer module.



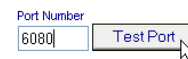
- a. Click **SKIP** when asked to register.
  - b. Click **NO** if asked if you want to use the same settings you used last time.
  - c. Click **SKIP** when prompted to enter a password.
  - d. Click **NO** when asked if you want the customer module to auto-reconnect.
  - e. Click **NO** when asked if you want to use your existing configuration file.
  - f. Enter the public address to your workstation. Example: **123.456.789.0**
  - g. Enter the public port you opened in your router. Example: **6080**
  - h. Click **NO** when asked if you will be using the Repeater.
  - i. Click **NO** when asked if you want to use the encryption plugin.
  - j. Click **NO** when asked if you want the module to load it's configuration from a web server.
  - k. Click **NO** when asked if you want to use the on-screen timer.
  - l. Click **DEFAULT** when asked to enter URL to your tools website.
  - m. Close the “Customer Modules” folder that opened during the creation process. We will not need it at this point. The support module named OneClick.exe in the folder is the file that your customer would run so you would normally copy it to a location accessible to your customer, such as your website and create a link to it on your support page or send it via email or on disk. But we are just testing your port so do not distribute this module (123.456.789.0 is not a valid address)
4. Run the “**Listen Port 6080 NO Encryption**” icon the creator added to the OneClick folder. This will run the viewer in listen mode and add an icon to your system tray beside the clock on your desktop. If you get an “Error Binding Socket” message, another service is already using this port and you will need to select a different port for OneClick.



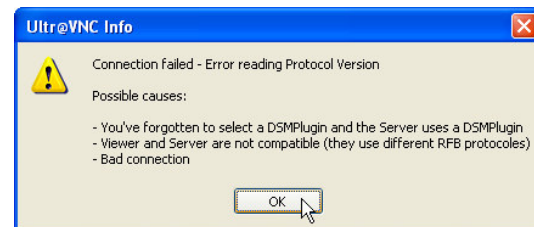
5. Run the “**Test your OneClick port**” icon in the OneClick folder. You must have the viewer running in listen mode (step 4 above) before testing the port (or before the customer runs your customer module). This will launch your web browser and take you to the port test page which will display your public IP address and allow you to enter the port number you wish to test.



- a. Enter the port number in the “port Number” box and click the “Test Port” button. Example: **6080**



If the port test passed you should get a popup from the listening Viewer that says “Connection Failed – Error reading protocol version”. The Viewer reports this as an error since the web-based test does not establish an actual VNC session.



If you do not get the popup from the listening Viewer, the port test failed to pass through your router, gateway or firewall and you will need to check your port forwarding settings. If your workstation is behind multiple routers, each router must forward to the next router in the path between your workstation and the router with the public IP address. The router connected directly to your workstation then forwards to the workstation.

6. If the port test passed successfully, you are now ready to build your permanent customer module. Run the “Create a Customer Module” program and select the options, address and port you wish to use. If you are using a DSL or cable connection with a dynamic IP address we recommend using a Dynamic DNS provider such as no-ip.com or dyndns.com to allow you to use a static DNS name in your customer module.

7. Copy the OneClick.exe file from the customer modules folder to a location accessible to your customer such as your website and create a link to it on your support page or send it via email or on disk. You may rename the file if you wish.



8. Run the Viewer. If you will not be using the repeater, ensure you have the Viewer running in listen mode. You should have a Viewer icon in the system tray near the clock on your desktop.



If you will be using the repeater, use the icon named “Connect to Repeater NO Encryption” or “Connect to Repeater WITH Encryption” in the OneClick folder. You will need to enter the same ID number you used when you built your customer module.



9. Have your customer run the OneClick.exe file to connect to your computer. If the customer is on the same LAN you may have to use an internal (private) address in your customer module since not all routers will allow you to connect to an internal workstation using a public address from inside the same LAN.



## Understanding IP Addresses, Ports, Port Forwarding, Port Mapping etc.

### What is an IP address?

IP (internet protocol) addresses are used to identify computers and other electronic equipment on the internet. Every device connected to the internet must have a public IP address to communicate with any other device over the internet just as every telephone that communicates with another telephone over the public telephone service must have a public telephone number.

### What is a DNS or DDNS name or address?

DNS (domain name system) and DDNS (dynamic domain name system) names are used to find an IP address as you use a telephone book or information service to find a telephone number. Programs such as internet explorer do a DNS look-up using a DNS service to find the IP address of the URL (uniform resource locator) address you enter in the address field. If you enter the actual IP address directly, no DNS look-up is needed or performed. You do not need to enter the URL to connect to a web server, for example you can enter HTTP://129.168.0.1 to connect to the web server built into your router (if that's the address to your router of course). DNS is used for static (non-changing) IP addresses and DDNS providers are used for dynamic (can change) IP address similar to DHCP (dynamic host configuration protocol). Unless you requested a static IP address from your ISP it is probably dynamic. Support for DDNS is built into most routers.

### What is an ISP (Internet Service Provider)

An ISP provides access to the internet like a telephone company provides access to telephone service.

### What is a Router or Gateway?

A router is similar in operation to a telephone PBX (Private Branch Exchange) in an office. It allows multiple computers to connect using the same internet connection as a PBX allows multiple telephones in the office to be connected to the same public telephone number.

A Router is a privately owned network system to reduce the total number of public IP addresses needed from an ISP. Without a router, a company would need a public IP address for every employee with a computer.

A PBX is a privately owned telephone switching system used to reduce the total number of public telephone numbers needed from the telephone company. Without a PBX, a company would need a public telephone number for every employee with a telephone.

### What is a Public or WAN IP Address?

Public internet addresses are outside address like public outside line telephone numbers. Every computer that accesses the internet must communicate through public internet address just as every telephone that accesses the public telephone system must communicate through a public telephone number (outside line).

### What is a Private IP or Internal IP Address?

Private IP addresses are like internal PBX telephone numbers. They can only be reached from inside the same network as a telephone extension can only be reached from inside the same PBX. Just as dialing extension 101 will connect someone inside a building to someone else inside the same building and not to another company, connecting to 192.168.0.101 will connect to a workstation inside the same network and not to a computer across the internet. Private IP addresses are blocked by your ISP and will not be forwarded or connected to the internet just as a PBX will not forward a dialed extension to the phone company.

*Private IP addresses should not be confused with what is referred to as unlisted or private telephone numbers, which use public phone numbers but aren't listed or published in the phone book.*

Private IP addresses are ranges of IP addresses reserved for internal (private) network communications by the IANA (Internet Assigned Numbers Authority). The following ranges of IP addresses are reserved and are not routable:

10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255, 192.168.0.0 - 192.168.255.255, 169.254.0.0 - 169.254.255.255

### What are Port Numbers?

Port numbers are like internal PBX telephone extensions. They are used to connect to a specific program, private IP address or computer as a PBX telephone extension is used to connect to a specific person, telephone or desk.

### What is Port Forwarding or Port Mapping?

Port forwarding refers to the process of instructing your router or gateway to forward data coming in on a specific public port through to a specific private computer or program as programming a PBX instructs it to forward a specific telephone extension to specific a person or telephone.

### What is DMZ (demilitarized zone)?

DMZ is similar to port forwarding or port mapping but on a larger scale. It forwards ALL incoming data to a specific private or internal computer, not just data on specific ports. This is effectively the same as connecting to the internet without a router, gateway or firewall and is not recommended since it subjects the internal computer to all incoming data on any port with little or no protection from hacking attempts.

**Notes:**