Quick Start Guide

1. Run the RemoteZilla-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 let's use port **831** 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 will familiarize you with creating a customer module to 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.

- **Registered** Name - Enter the name as shown on your invoice or registration email.
  If the name does not match the one registered, the customer modules will expire.
  If you have not registered yet, leave it set to "* Unregistered Trial *".

- **Registration Key** - Enter the registration key exactly as show in your registration email.
  If you copy and paste ensure you do not copy blank spaces. If you have not registered yet, leave it set to "0"**.**

- **Window Title** - Normally you would enter the company name you want displayed in the customer modules and timer but this is only a non-working test module so leave it set to the default until you build a permanent customer module.

- **IP/DNS Address** – Enter: **TEST**
  Normally you would enter the public (WAN) address to your router (*or workstation*), not your website unless you are using your workstation as your web server. This can be a DNS name, DDNS name or an IP address. Since we are only testing port forwarding at this point enter: **TEST**

- **TCP Port Number** - Enter: **831**
  This is the public port you opened in your router.

- Click the **Create Customer Module** button. The only options needed to create a working customer module are the IP/DNS address and port number. Everything else is optional.

- Click **NO** if asked if you want to register now (valid registrations won't see this).

- Click **YES** when asked if this machine will be listening for incoming connections or running the proxy software on port 831.

- You will then be given information on the location where the Shortcut to the Listen program was created. This is will be in the Advantig RemoteZilla folder on the desktop regardless of where you installed. Click the **OK** button to close it.

- **Delete** the **Customer_TEST_830_Direct.exe** file *("TEST" is not a valid internet address)* we are just setting up to test your port and find your public internet address to create a real customer module.

- **Close** the "**Customer Modules**" folder that opened during the creation process. We will not need it at this point. The customer support modules are named:
  Customer_<your address>_<your port>_<connect mode>.exe
  and created in the customer modules folder. They are the files that your customers will run when they need support 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.

- Run the "**RemoteZilla Listen Port 831 NO Encryption**" shortcut the creator added to the Advantig RemoteZilla folder on your desktop. 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 or you already have a listening viewer running and you will need to close the other program or select a different port for RemoteZilla. Only one program or service can listen to a port at a time.

- Right-Click the Listening RemoteZilla Viewer Icon in the system tray and select "**Test Listening Port** " from the menu. This will give you a popup box with some basic information about your system and instructions.
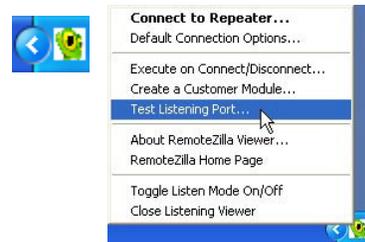
- **Click the OK button**. This will launch your web browser and take you to the port test page, which will display your public IP address and Private IP address and test your port. At this point the port has NOT been tested. You have to click the OK button to proceed to the port test page before the test will begin.

- If the port test passed you should get a popup from the listening Viewer like the one shown below that says "Port Test Passed. Successfully received the port test connection". The web-based test does not establish an actual RemoeZilla session it only tests the port.
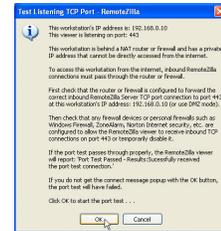
  If you do not get the popup from the listening Viewer, the port test failed to pass through your router, gateway or firewall and you will need to check your port forwarding settings. If your workstation is behind multiple routers, each router must forward to the next router in the path between your workstation and the router with the public IP address. The router connected directly to your workstation then forwards to the workstation.
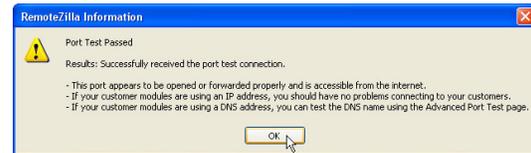
  If the web page reports a successful connection but you do not get the popup, it means another program accepted the connection instead of your listening viewer and the port test did not pass, you will need to troubleshoot your settings. In some environments, the public address shown and tested on the port test page is not the IP address your inbound data uses. In this situation you will need to use the advanced port test page and enter the correct IP address.

- **Click the OK button** to close the port test popup.

If the port test did not pass, you will need to troubleshoot your settings. In some environments, the public address shown and tested is not the IP address your inbound data uses. In this situation you will need to use the advanced port test page and enter the correct IP address.

If the port test passed successfully, you are now ready to build a working customer module.

How to build a working customer module

- o Replace TEST in the IP/DNS box with the public IP address shown on the port test page.
- o Click the Create Customer Module button.

Congratulations, you're finished and now have a working customer module. To connect to a remote computer be sure the viewer is (still) running in listen mode as you did to test your port and run the customer module on the machine you wish to remote control. You can put the customer module on your website or email it to your customer. If you decide to email it, be sure to zip it first or rename the extension from .exe to .dat and have the customer rename it back to .exe before they try to run it as most email systems block executable (.exe) file attachments.

The simplest way to get the file to your customer is to put it on your website and add a link to it on a web page so the customer only has to click the link to run the file.

See the Creator Help (RemoteZilla-Creator.pdf) file in the RemoteZilla folder to view detailed information about settings and customization options available.

If you require further assistance visit   **http://www.remotezilla.com/contact** for our current contact information or send email to   **support@remotezilla.com**

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.