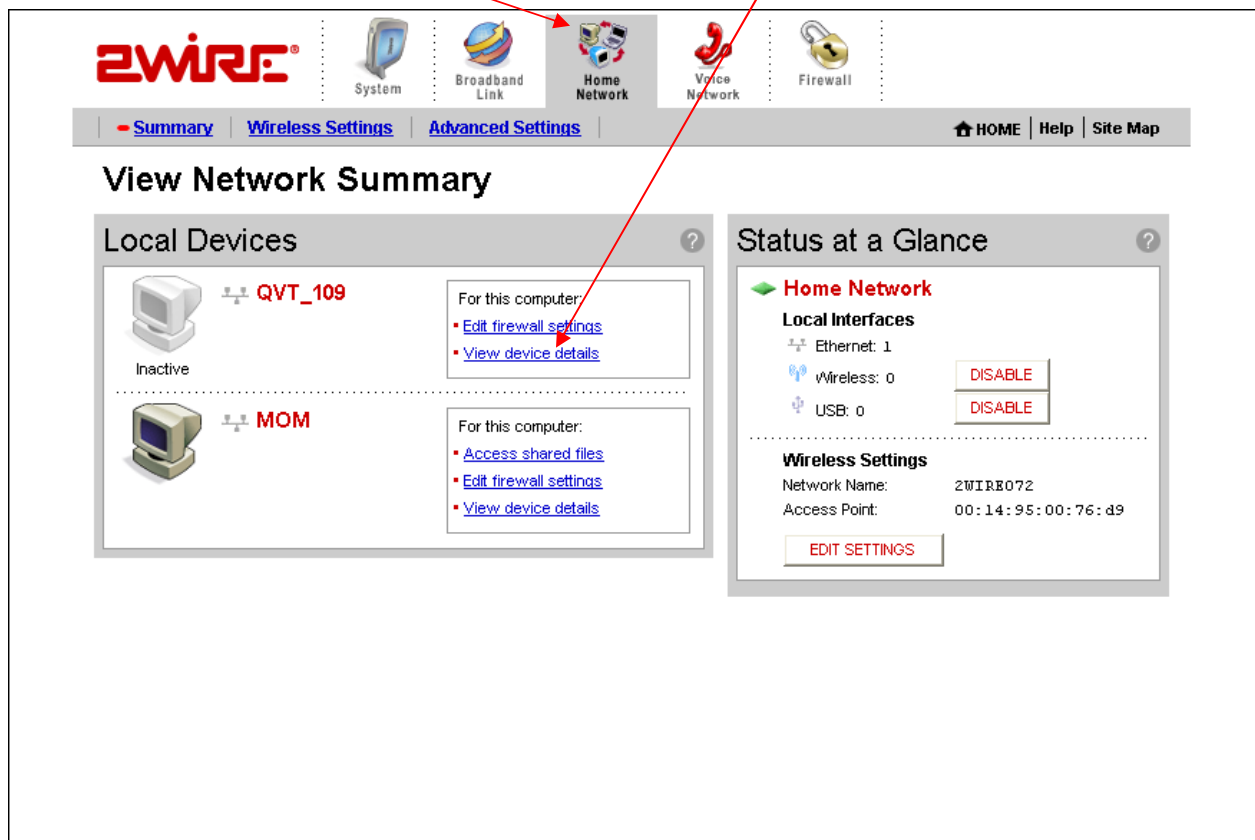


How to Setup Port forwarding on 2Wire routers (AT&T)

Open a web browser like Internet Explorer or Firefox. Enter the IP address of your router in the address bar of your browser. By default the IP address should be 192.168.1.254

Select [Home Network](#) and check for the DVR's IP address in Local Devices.

Note: You may rename the device by clicking on [View Device Details](#).



The screenshot displays the 2Wire router's web management interface. At the top, the 2Wire logo is on the left, and navigation icons for System, Broadband Link, Home Network, Voice Network, and Firewall are in the center. Below these are tabs for Summary, Wireless Settings, and Advanced Settings. The main content area is titled "View Network Summary" and is divided into two panels: "Local Devices" and "Status at a Glance".

The "Local Devices" panel lists two devices: "QVT_109" (Inactive) and "MOM". For each device, there are links for "Edit firewall settings" and "View device details". A red arrow points from the text above to the "View device details" link for the "QVT_109" device.

The "Status at a Glance" panel shows the "Home Network" status. Under "Local Interfaces", it lists "Ethernet: 1", "Wireless: 0", and "USB: 0", each with a "DISABLE" button. Under "Wireless Settings", it shows "Network Name: 2WIRE072" and "Access Point: 00:14:95:00:76:d9", with an "EDIT SETTINGS" button below.

Click the **Firewall** button.



The screenshot shows the Qwest router configuration interface. At the top, there are four main navigation buttons: System, Broadband Link, Home Network, and Firewall. A red arrow points from the text 'Click the Firewall button.' to the Firewall button, which is also circled in red. Below the navigation bar is a menu with links: Summary, Password, Date and Time, Details, Status, WAN Status, LAN Status, HOME, and Site Map. The main content area is divided into two columns. The left column contains three sections: '2700HG-D Gateway' with software version 4.25.19-QT01 and a 'Password Not Set' warning; 'Broadband Link' showing connection speeds of 3072 kbps incoming and 640 kbps outgoing; and 'Home Network Computers' with a list of four computer icons. The right column contains two sections: 'Firewall' which is 'Active' and has a 'View firewall summary' link; and 'Wizards' with an 'Advanced Configuration Settings' link.

Click the [Firewall Settings](#) button.



View Firewall Summary

Firewall Settings



Firewall Active

The firewall actively blocks access of unwanted activity from the Internet. If you are using an application that requires you to open a port in your firewall, you may do so by clicking Firewall Settings above.

Current Settings: Custom

| Device | Allowed Applications |
|----------|----------------------|
| DJGFP871 | BitTorrent |

[VIEW DETAILS](#)

Use the [Select a computer](#) box to choose the DVR to forward ports to. This box contains a list of device names or IP addresses that are visible on your network. Click the [Add a new user-defined application](#) link.

zWIRE System Broadband Link Home Network Voice Network Firewall

Summary **Firewall Settings** Advanced Settings HOME Help Site Map

Edit Firewall Settings

Settings

By default, the firewall blocks all unwanted access from the Internet. You can allow access from the Internet to applications running on computers inside your secure home network by enabling firewall pinholes. Opening firewall pinholes is also known as opening firewall ports or firewall port forwarding. To do this, associate the desired application with the computer below. If you cannot find a listing for your application, you can create a user-defined application profile. (To create a user-defined profile, you will need to know protocol and port information.)

- [View firewall details](#)
- [Reset all firewall settings](#)

To Allow Users Through the Firewall to Hosted Applications...

- Select a computer**
Choose the computer that will host applications through the firewall:
- Edit firewall settings for this computer:**
 - Maximum protection** – Disallow unsolicited inbound traffic.
 - Allow individual application(s)** – Choose the application(s) that will be enabled to pass through the firewall to this computer. Click ADD to add it to the Hosted Applications list.
 - All applications:
 - Age of Empires
 - Age of Kings
 - Age of Wonders
 - Aliens vs Predator
 - Anarchy Online
 - Asheron's Call
 - Baldur's Gate
 - BattleCom
 - Battlefield Communicator
 - Black and White
 - [Add a new user-defined application](#)
 - Hosted Applications:**
 -
 -
- Allow all applications (DMZplus mode)** – Set the selected computer in DMZplus mode. All inbound traffic, except traffic which has been specifically assigned to another computer using the "Allow individual applications" feature, will automatically be directed to this computer. The DMZplus-enabled computer is less secure because all unassigned firewall ports are opened for that computer.

Note: Once DMZplus mode is selected and you click DONE, the system will issue a new IP address to the selected computer. The computer must be set to DHCP mode to receive the new IP address from the system, and you must reboot the computer. If you are changing DMZplus mode from one computer to another computer, you must reboot both computers.

We will list a series of lines here that will show you exactly how to forward the ports you need to forward (**SEE DVR NETWORK INFO**). Go ahead and enter the DVR ports into the [Edit Application](#) menu and then click [Add Definition](#).

SBC System Broadband Link Home Network Firewall

Summary **Firewall Settings** Advanced Settings HOME Help Site Map

Edit Application

Settings

Profile Name
Enter a name for the application profile that you are creating.

Application Name:

Definition
Choose a protocol and enter the port(s) for this application, then click **ADD DEFINITION** to add the definition to the Definition List. If the application requires multiple ports or both TCP and UDP ports, you will need to add multiple definitions.

Note: In some rare instances, certain application types require specialized firewall changes in addition to simple port forwarding. If the application you are adding appears in the application type menu below, it is recommended that you select it.

Protocol: TCP UDP

Port (or Range): From: To:

Protocol Timeout (seconds): TCP default = 86400
UDP default = 600

Map to Host Port: Default = the same port as defined above.

Application Type:

Click the [Back](#) button

NOTE: Repeat for all ports.

Select the DVR from the [Select a computer](#) menu. Select the applications you just created in the [Applications](#) list and click the [Add](#) button to move them to the [Hosted Applications](#) box.

2WIRE® System Broadband Link Home Network Voice Network Firewall

Summary - **Firewall Settings** Advanced Settings HOME Help Site Map

Edit Firewall Settings

Settings

By default, the firewall blocks all unwanted access from the Internet. You can allow access from the Internet to applications running on computers inside your secure home network by enabling firewall pinholes. Opening firewall pinholes is also known as opening firewall ports or firewall port forwarding. To do this, associate the desired application with the computer below. If you cannot find a listing for your application, you can create a user-defined application profile. (To create a user-defined profile, you will need to know protocol and port information.)

- [View firewall details](#)
- [Reset all firewall settings](#)

To Allow Users Through the Firewall to Hosted Applications...

1 Select a computer
Choose the computer that will host applications through the firewall:

2 Edit firewall settings for this computer:

- Maximum protection** – Disallow unsolicited inbound traffic.
- Allow individual application(s)** – Choose the application(s) that will be enabled to pass through the firewall to this computer. Click ADD to add it to the Hosted Applications list.

All applications:

Hosted Applications:

Age of Empires
Age of Kings
Age of Wonders
Aliens vs Predator
Anarchy Online
Asteron's Call
Baldur's Gate
BattleCox
Battlefield Communicator
Black and White

ADD REMOVE

[Add a new user defined application](#)

- Allow all applications (DMZplus mode)** – Set the selected computer in DMZplus mode. All inbound traffic, except traffic which has been specifically assigned to another computer using the "Allow individual applications" feature, will automatically be directed to this computer. The DMZplus-enabled computer is less secure because all unassigned firewall ports are opened for that computer.

Note: Once DMZplus mode is selected and you click DONE, the system will issue a new IP address to the selected computer. The computer must be set to DHCP mode to receive the new IP address from the system, and you must reboot the computer. If you are changing DMZplus mode from one computer to another computer, you must reboot both computers.

DONE

When you are finished, click the [Done](#) button at the bottom of your screen.

And that is it! You are done!