

## Qwest® Advanced Networking Modem with Wireless: 2Wire® 2700 HG

### Firewalls How to Configure Firewall Settings

The Qwest® Advanced Networking Modem with Wireless: 2Wire® 2700 HG firewall “Settings” page allows you to configure the firewall so application-specific data can pass through to a selected computer.

For example, you must configure your firewall to host an application (e.g., a Web server) on your network for Internet users to access.

**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](#)

**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.

**Applications:**

All

**Games**

AudioVideo

Messaging and Internet

Phone

Servers

Other

User-defined

[Add a new user-defined application](#)

[Edit or delete user-defined application](#)

UPDATE APPLICATION LIST

Age of Empires  
Age of Kings  
Age of Wonders  
Baldur's Gate  
BattleCox  
Battlefield Communicator  
Dark Reign  
Delta Force 3  
Descent 3  
Descent Freespace  
Diablo (1.074)  
Diablo I  
Diablo II  
DirectX Games  
Doom

**ADD >**

**< REMOVE**

**Hosted Applications:**

Half Life  
MechWarrior 3

**Allow all applications (DMZplus mode)** – Set the selected computer in DMZplus mode. All inbound traffic will be directed to this computer. The DMZplus enabled computer is less secure because all firewall ports are opened for that computer.

Current DMZplus computer: **Bad**

**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**



To configure your firewall:

1. From the "Select a computer" drop-down menu, select the computer.
2. Select the **Allow individual application(s)** radio button.
3. Select an application profile.  
Note: To sort applications by category, select the oval next to the category name. Select "ALL" to see a list of all application profiles.
4. Select the **ADD >** button.
5. Select the **DONE** button.

To stop an application routed to the selected computer, you must remove the application profile name from the "Hosted Applications" list.

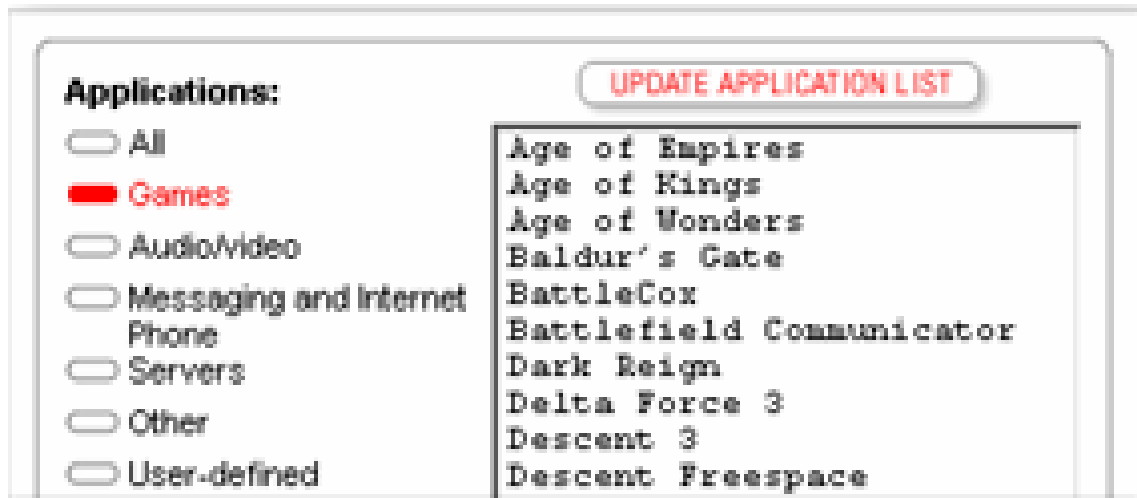
1. Select the application profile name on the "Hosted Applications" list.
2. Select the **< REMOVE** button.

Note: Although there's no limit to the number of applications that one computer can host, the firewall allows only one application profile in use at a time. For example, if a hosted application appears in the "Johnny" profile, it can't be added to another computer's list until it's removed from the "Johnny" profile.

Qwest® Advanced Networking Modem with Wireless:  
2Wire® 2700 HG

Firewalls  
How to Update the Application Profile List

If the application you want to host doesn't appear in the "Application Profile" list, you may need to update the list of applications from the firewall "Settings" page.



If an update is available, the **UPDATE APPLICATION LIST** button appears above the list of application profiles. To update the list of applications, select that button.

If the application you want to host is not listed under the **UPDATE APPLICATION LIST** button, you may need to create your own application profile.

**Qwest® Advanced Networking Modem with Wireless:  
2Wire® 2700 HG**

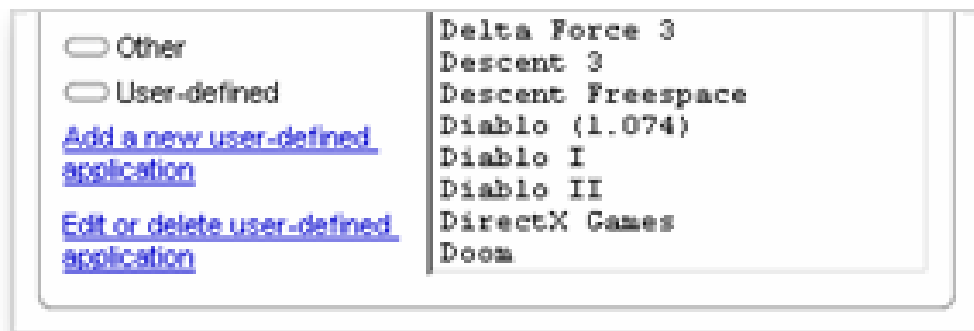
**Firewalls  
How to Create and Add a New Application Profile**

After updating the “Application Profile” list, and the application you want to host doesn’t appear, you can add it manually from the firewall “Settings” page.

An application profile allows application-specific data to pass through your system’s configured firewall. The typical use of this feature is when the selected application is new, or is an updated version that needs to pass data to a given computer.

**Add a New Application Profile**

To add an application manually, select the **Add a new user-defined application** link.



- To determine the configuration parameters needed to set up your application profile, consult the documentation provided with the application or visit the application manufacturer’s Web site.
  - The documentation for the application you want to host includes the correct protocols and ports necessary for the application to function properly.
  - To set up the new profile, read the included information about Network Address Translation (NAT), firewall, port mapping, application hosting, or TCP and UDP ports.
- NAT is a firewall software feature that blocks application data. For your application to work through NAT, you need to create an application profile that properly configures your firewall.

## Create a New Application Profile

The “Add Application Profile” page allows you to create an application profile for hosted applications not included in the pre-defined “Application Profile” list.


### 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.

<b>Protocol:</b>	<input checked="" type="radio"/> TCP	<input type="radio"/> UDP
<b>Port (or Range):</b>	From: <input type="text"/>	To: <input type="text"/>
<b>Protocol Timeout (seconds):</b>	<input type="text"/>	TCP default = 86400 UDP default = 600
<b>Map to Host Port:</b>	<input type="text"/>	Default = the same port as defined above.
<b>Algorithm:</b>	<input type="text" value="None (Default)"/> 	

Click **ADD** 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.

**ADD**

**DONE**

1. Enter a profile name in the **Application Name** field. We recommend using the name of the application (e.g., “ICMI Messenger” or “Redwing Game Server”).

2. In the **Definition** window, create a definition for your application. A “definition” is a series of protocol-specific ports allowed through the firewall as specified by the manufacturer.
  - **Protocol:** Enter either the TCP or UDP protocol unless the application uses both. If both protocols are required, you must create a definition for each.
  - **Port (or Range):** Enter the chosen port or port range used by the application. For example, “Application A” may only require passing through TCP Port 500, whereas “Application B” may require passing through all TCP Ports from 600 to 1000.
  - **Protocol Timeout:** Amount of time (in seconds) a connection in the specified range remains open without data transfer.
    - After establishing a port connection, the sender and receiver usually determine when the session is finished and the connection is closed.
    - If the connection is left open and data transfer stops, the system closes the connection and reclaims the resources to protect your network.
    - An advanced feature allows you to lengthen the default value timeout, if the system closes the application during normal operation (e.g., a long pause between data transfer).
  - **Map to Host Port:** When set, provides the mapping offset to the local computer. For example, if this value is set to 4000 and the range opened is 100 - 108, the forwarded data is sent to 4000, the first value in the range. Subsequent ports are mapped accordingly (e.g., 101 is sent to 4001, 102 is sent to 4002).
3. Select **ADD** to add values to the profile definition list at the bottom of the screen. You must select **ADD** to retain the defined values.
4. Repeat the previous step for each port or range of ports required for the application profile.
5. Select **DONE**.

**Qwest® Advanced Networking Modem with Wireless:  
2Wire® 2700 HG**

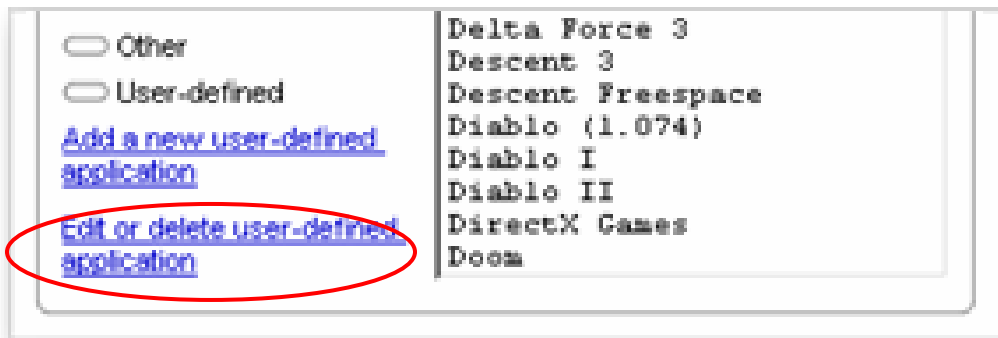
**Firewalls  
How to Edit or Delete Application Profiles**

An application profile allows application-specific data to pass through your system's configured firewall.

You can edit or delete application profiles manually from the firewall "Settings" page.

- Use this to delete applications no longer installed on your home network.
- You cannot modify or delete any pre-defined applications on the list; only applications you've defined.

1. To edit or delete an application profile, select the **Edit or delete a user-defined application** link.

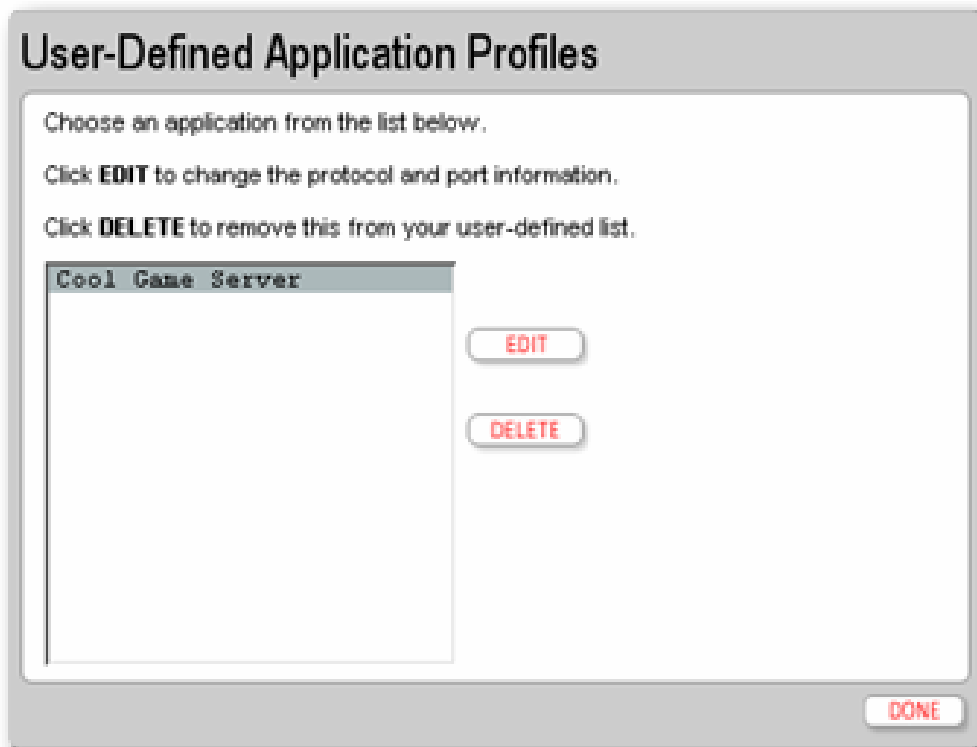


2. To edit application profiles you've created:

- Select the profile from the list.
- Select the **EDIT** button.
- Make selections on the "Edit Application Profile" page.

3. To delete an application profile:

- Select the application profile from the list.
- Select the **DELETE** button.





## Qwest® Advanced Networking Modem with Wireless: 2Wire® 2700 HG

### Firewalls How to Configure DMZplus

**DMZplus**, a special firewall mode used for hosting applications, is an alternative to using the “Allow individual application(s)” option, in the event those hosting applications are operating improperly.

Caution: A computer in **DMZplus** mode is less secure because all available ports are open and all incoming Internet traffic is directed to this computer.

You can configure **DMZplus** for only one computer on your home network at a time.

- The “Firewall Settings” page allows you to enable **DMZplus** and select which computer runs in **DMZplus** mode.
- **DMZplus** mode protects your computer using your system firewall, although it’s connected to the Internet directly.
- The firewall’s Stateful Packet Inspection engine inspects all traffic and continues to block known hacker attacks.
- Use the **DMZplus** mode with caution since all filtered traffic is forwarded to the designated computer.
- Use the “Allow individual application(s)” option to support access from Internet applications on your network.

In **DMZplus** mode, the designated computer:

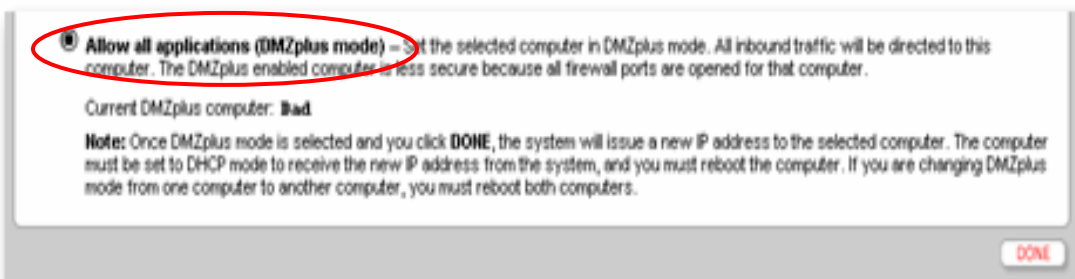
- “Shares” your Router Address (system’s IP address).
- Appears directly connected to the Internet.
- Has all unassigned TCP and UDP ports opened and pointed to it.
- Is able to receive unsolicited network traffic from the Internet.

To configure a computer on your network for **DMZplus** mode:

1. Select the computer from the “Select a computer” drop-down list.



2. Select the **Allow all applications (DMZplus mode)** radio button.



3. Select **DONE**.
4. Access the selected computer and complete **Computer Set Up**.

### Computer Set Up

1. Configure the computer for DHCP, if it's not already.
2. **Restart** the computer to receive a special IP address from the system, and to forward all unassigned TCP and UDP ports.



## Qwest® Advanced Networking Modem with Wireless: 2Wire® 2700 HG

### Firewalls How to Disable DMZplus

To disable **DMZplus** mode for your system:

1. Select the computer on which you want to disable **DMZplus**.
2. Select **Maximum Protection**.
3. Select **DONE**.
4. Access the computer in **DMZplus** mode and complete **Computer Set Up**.

#### Computer Set Up

1. If the computer continues to obtain an IP address automatically, proceed to Step 3.
2. If the computer has an existing static IP address, create a valid static IP address.
3. **Restart** the computer.



## Qwest® Advanced Networking Modem with Wireless: 2Wire® 2700 HG

### Firewalls How to Use Advanced Firewall Configuration

*Caution:*

*Only an experienced network administrator with advanced knowledge of firewalls and networking should modify advanced settings.*

Advanced firewall configuration allows advanced users to further configure the system software firewall.

- The firewall doesn't automatically allow inbound traffic to pass through to the network.

If a protocol or application type is allowed via the Advanced Configuration settings, the firewall still checks and blocks all unsolicited Internet traffic unless the application profile configures the firewall to allow the traffic.

- Firewall filtering takes precedence over application hosting.

By disabling incoming traffic, you may disable support for hosted applications requiring that type of inbound communication.

1. Select the **Inbound** checkbox to allow the corresponding protocol to pass through the firewall from the Internet to the network.
2. Select the **Outbound** checkbox to allow the traffic from the network to pass through the firewall to the Internet.
3. Select the **SAVE** button for changes to take effect.

## Settings

### Security

Check to enable the features below:

Stealth Mode	<input type="checkbox"/>
Strict UDP Session Control	<input type="checkbox"/>

### Inbound and Outbound Control

Checking the box allows the associated traffic type through the firewall.

#### Outbound

HTTP	<input type="checkbox"/>
HTTPS	<input type="checkbox"/>
FTP	<input type="checkbox"/>
Telnet	<input type="checkbox"/>
SMTP	<input type="checkbox"/>
DNS	<input type="checkbox"/>
POP3	<input type="checkbox"/>
IMAP	<input type="checkbox"/>
NNTP	<input type="checkbox"/>
IRC	<input type="checkbox"/>
H323	<input type="checkbox"/>
All Other Protocols	<input type="checkbox"/>

#### Inbound

Remote Management	<input type="checkbox"/>
Remote Configuration	<input type="checkbox"/>

SAVE

CANCEL