How to open ports in Win7 Firewall

Open the Firewall from ControlPanel > Windows Firewall. In the left side panel select Advanced Settings



The advanced settings should look something like this:

Select Inbound Rules

@	Windows Firewall with Advanced Security - C					
File Action View Help Image: Strain S	Inbound Rules					Actions
Connection Security Rules	Name Daemonu.exe Daemonu.exe Daemonu.exe BranchCache Content Retrieval (HTTP-In) BranchCache Hosted Cache Server (HTT BranchCache Peer Discovery (WSD-In) Connect to a Network Projector (TCP-In) Connect to a Network Projector (TCP-In) Connect to a Network Projector (WSD Ev Connect to a Network Projector (WSD Ev)	Group BranchCache - Content Retr BranchCache - Hosted Cach BranchCache - Peer Discove CheckPoint.VPN Connect to a Network Proje Connect to a Network Proje Core Networking Core Networking Core Networking	Profile Private Private All All All Private Domain Private Private All All All All All All All All All	Enabled No No No Vo Yes No No No No Yes Yes Yes	~	Inbound Rules Image: New Rule Image: Filter by Profile Image: Filter by Group Image: Filter by Group View Image: Refresh Image: Export List Image: Help
< >>	<			>		

<i>₽</i>	New Inbound Rule Wizard
Rule Type Select the type of firewall rule to c	create.
Steps: Protocol and Ports Action Profile Name	What type of rule would you like to create? Pargaram Rule that controls connections for a program. Image: Controls connections for a TCP or UDP pot. Predefined: BranchCache - Content Retrieval (Uses HTTP) Rule that controls connections for a Windows experience. Outcom Custom rule.

A 'Port' rule should be created. Click Next

<i>@</i>	New Inbound Rule Wizard					
Protocol and Ports						
Specify the protocols and ports to which this rule applies.						
Steps:						
Rule Type	Does this rule apply to TCP or UDP?					
Protocol and Ports	• <u>I</u> CP					
 Action 						
Profile						
 Name 	Does this rule apply to all local ports or specific local ports?					
	○ <u>All local ports</u>					
	Specific local ports: 4606, 4607					
	Example: 80, 443, 5000-5010					
	< <u>B</u> ack <u>N</u> ext > Cancel					

In this case we want TCP and Specific local ports. For the Specific local ports: enter 4606 and 4607 separated by a comma. Click Next

@	New Inbound Rule Wizard	×
Action Specify the action to be taken wh	en a connection matches the conditions specified in the rule.	
 Rule Type Protocol and Ports Action Profile Name 	What action should be taken when a connection matches the specified conditions? Image: Connection Connection that are protected with IPsec as well as those are not. Image: Connection Connection that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security and node. Image: Connection Co	

We want to "Allow the connection" Click Next

<i>₽</i>	New Inbound Rule Wizard					
Profile Specify the profiles for which this	rule applies.					
Specify the profiles for which this Steps: Protocol and Ports Action Profile Name	 When does this rule apply? ✓ Domain Applies when a computer is connected to its corporate domain. ✓ Private Applies when a computer is connected to a private network location, such as a home or work place. ✓ Pyblic Applies when a computer is connected to a public network location. 					
	< Back Next > Cancel					

Select the appropriate options here. Normally all three options would be checked. Click Next

•	New Inbound Rule Wizard
lame	
pecify the name and descripti	on of this rule.
teps:	
Rule Type	
Protocol and Ports	
Action	
Profile	Name:
Name	DeviceMaster Driver and Port Vision
	Description (optional):
	DeviceMaster Driver and PortVision both use 4606. The diagnostic port of the DeviceMaster is port 4607

Supply a name for the rule. Here we entered DeviceMaster and PortVision. The Description is optional but for future reference it may be helpful.

<i>@</i>	Windows Fi	rewall with Advanced Sec	urity			- 🗆 🗙
<u>File Action View H</u> elp						
🗢 🔿 🗹 🔃 🗟 🖬	Inhound Rules					Actions
Inbound Rules	Name	Group	Profile	Enabled	^	Inbound Rules
🛼 Connection Security Rules	OeviceMaster Driver and PortVision		All	Yes		🧱 New Rule
Monitoring	Daemonu.exe	monu.exe Pr	Private No Private No All No	No		
	BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr				
	BranchCache Hosted Cache Server (HTT	ache Server (HTT BranchCache - Hosted Cach	All	No		▼ Filter by Group
	BranchCache Peer Discovery (WSD-In) BranchCache - Peer Discove	All	No		View	
	CheckPoint.VPN	CheckPoint.VPN	All	Yes		Q Refresh
	Connect to a Network Projector (ICP-In) Connect to a Network Projector (TCP-In) Connect to a Network Projector (WSD Ev Connect to a Network Projector (WSD Ev Connect to a Network Projector (WSD Ev	Connect to a Network Proje Connect to a Network Proje	k Proje Private k Proje Domajn	No No		Export List
		Domain	No		P Help	
	Connect to a Network Projector (WSD Ev	nnect to a Network Projector (WSD Ev., Connect to a Network Proje., Private., nnect to a Network Projector (WSD Ev., Connect to a Network Proje., Private., nnect to a Network Projector (WSD Ev., Connect to a Network Proje., Domain	No No		DeviceMaster Driver and PortV	
	Connect to a Network Projector (WSD Ev		Domain	No		Disable Rule
	Connect to a Network Projector (WSD-In)	Connect to a Network Proje	All	No		K Cut
	Ocre Networking - Destination Unreacha	Core Networking	All	Yes		
	Ocre Networking - Destination Unreacha	Core Networking	All	Yes	~	
× >	<			>		

The new rule should now be displayed at the top of the center panel and also in the right side panel.

Close the Advanced settings.