

How to open up TCP, UDP Ports and Ping Ports on Windows

system?

(Firewall)

June-29-2020, Version V.0

Contact information: support@dolphinpos.com

Index	Page#
Opening TCP or UDP Port	2-5
Opening ICMP echo mode (Ping)	6-11

Firewall changes

1. From the "PC" go to → Control Panel\System and Security\Windows Defender Firewall

Click **advanced settings (on the left side**). The Windows Firewall and Advanced Security screen appears.



2. Click "Inbound Rules".

(On the left side, under windows firewall ... "Inbound Rules")

3. Click "**New Rule**". The New inbound Rule Wizard appears. (On the right side, under Inbound rules …"New Inbound Rules")

Firewall rule Application

🗢 🄿 🙍 📰 🔂 📰							
🔗 Windows Defender Firewall witl	Inbound Rules Actions						
Cuthound Rules	Name	Group	Profile	Enabled	Action ^	Inbound Rules	
Windows Defender Firewall with Choose and the second sec	Inbound Rules Vame UDP PORT 5984 GetMicrosoft.AAD.BrokerPlugin_1000.171 GetMicrosoft.MicrosoftEdge_42.17134.10 GetMicrosoft.MicrosoftEdge_42.17134.1.0 GetMicrosoft.MicrosoftEdge_42.17134.1.0 GetMicrosoft.PPIProjection_10.0.17134.1 GetMicrosoft.PPIProjection_10.0.17134.1 GetMicrosoft.Windows.CloudExperience GetMicrosoft.Windows.CloudExperienc	Group @{Microsoft.AAD.BrokerPlu @{Microsoft.MicrosoftEdge @{Microsoft.WicrosoftEdge @{Microsoft.PPIProjection @{Microsoft.Windows.Clou} @{Microsoft.Windows.Clou} @{Microsoft.Windows.Cl	Profile All Domai Domai Domai All Public Domai Domai Domai Domai Domai Domai Domai Domai Domai	Enabled Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes	Action Allow Allow Allow Allow Allow Allow Allow Allow Allow Allow Allow Allow Allow Allow Allow Allow Allow Allow	Actions Inbound Rules Inbound Rule Filter by Profile Filter by State Filter by Group View Refresh Export List Help UDP PORT 5984 Disable Rule Cut Copy Delete	▲
		©FirewallAPI.dll, 80200 (78E1CD88-49E3-476E-B926 (78E1CD88-49E3-476E-B926 (78E1CD88-49E3-476E-B926 (78E1CD88-49E3-476E-B926 (78E1CD88-49E3-476E-B926 (78E1CD88-49E3-476E-B926 (78E1CD88-49E3-476E-B926 (78E1CD88-49E3-476E-B926)	AII AII AII AII AII AII AII AII	Yes Yes Yes Yes Yes Yes Yes Yes	Allow Allow Allow Allow Allow Allow Allow	Properties	

Click on "<u>Port</u>" (TCP or UDP depending on the desired local ports) and then click on "Next" button.



5. Choose either TCP or UDP and then enter the port numbers to open (like **5984**) and then click on "**Next**" button.

P New Inbound Rule Wizard		X						
Protocol and Ports	Protocol and Ports							
Specify the protocols and ports to whi	ich this rule applies.							
Steps:								
Rule Type	Does this rule apply to TCP or UD	99						
Protocol and Ports	TCP							
Action	O UDP							
Profile								
Name	Does this rule apply to all local po	rts or specific local ports?						
	All local ports Securities local and	Internal						
	Specific local ports:	5364						
		CABILITIA, 00, 445, 000/0010						
		< Back Next > Cancel						

6. The Action screen appears. Select "Allow the connection" and then click on "Next" button.



7. The Profile screen appears, make sure "Domain", "Private" and "public" should be selected and then click on "**Next**" button.



8. The Name screen appears. Enter a name and description for the rule (like TCP PORT 5984).Click **Finish**. The rule will be added.

-	
Mew Inbound Rule Wizard	
Name	
Specify the name and description of this n	ule.
Steps:	
 Rule Type 	
 Protocol and Ports 	
 Action 	
Profile	Name:
Name	TCP PORT 5984
	Description (optional):
	opening TCP PORT 5984 for Couch DB
	< Back Einish Cancel
	Carlos

Ping enabling for the inbound rule

1. From the "PC" go to → Control Panel\System and Security\Windows Defender Firewall

Click **advanced settings (on the left side**). The Windows Firewall and Advanced Security screen appears.



- 2. Click "**Inbound Rules**". (On the left side, under windows firewall ..."Inbound Rules")
- 3. Click "**New Rule**". The New inbound Rule Wizard appears. (On the right side, under inbound rules …"New Inbound Rules")

Firewall rule Application

🗢 🄿 🖄 📰 🗟 🛛 🖬						
🔗 Windows Defender Firewall witl	Nindows Defender Firewall with Inbound Rules					
Inbound Rules	Name	Group	Profile	Enabled	Action ^	Inbound Rules
Connection Security Rules	🔮 UDP PORT 5984		All	Yes	Allow	🐹 New Rule
> 🍇 Monitoring	@{Microsoft.AAD.BrokerPlugin_1000.171 @@{Microsoft.MicrosoftEdge_42.17134.1.0 @@{Microsoft.MicrosoftEdge_42.17134.1.0 @@{Microsoft.MicrosoftEdge_42.17134.1.0	@{Microsoft.AAD.BrokerPlu @{Microsoft.MicrosoftEdge @{Microsoft.MicrosoftEdge @{Microsoft.MicrosoftEdge	Domai Domai Domai Domai	Yes Yes Yes Yes	Allow Allow Allow Allow	▼ Filter by Profile ▼ Filter by State ▼ Filter by Group
	@@{Microsoft.PPIProjection_10.0.17134.1 @@{Microsoft.PPIProjection_10.0.17134.1 @@{Microsoft.Windows.CloudExperience	@{Microsoft.PPIProjection @{Microsoft.PPIProjection @{Microsoft.Windows.Clou @[Microsoft.Windows.Clou	All Public Domai	Yes Yes Yes	Allow Allow Allow	View
	@(Microsoft.Windows.CloudExperience @@(Microsoft.Windows.CloudExperience @@(Microsoft.Windows.CloudExperience @@(Microsoft.Windows.CloudExperience	@{Microsoft.Windows.Clou @{Microsoft.Windows.Clou @{Microsoft.Windows.Clou	Domai Domai	Yes Yes Yes	Allow Allow Allow	Help
	@@{Microsoft.Windows.CloudExperience @@{Microsoft.Windows.CloudExperience @@{Microsoft.Windows.CotlouExperience @@{Microsoft.Windows.Cortana_1.10.7.17 @@{Microsoft.Windows.Cortana_1.10.7.17 @@{Microsoft.Windows.Cortana_1.10.7.17 @@{Microsoft.Windows.Cortana_1.10.7.17 @@{Microsoft.Windows.Cortana_1.10.7.17 @@{Microsoft.Windows.Cortana_1.10.7.17 @@{Microsoft.Windows.Cortana_1.10.7.17 @@{Microsoft.Windows.Cortana_1.10.7.17} @Microsoft.Windows.Cortana_1.10.7.17} @@{Microsoft.Windows.Cortana_1.10.7.17} @{Microsoft.Windows.Cortana_1.10.7.17} @{Microsoft.Windows.Cortana_1.17} @{Micro	@{Microsoft.Windows.Clou @{Microsoft.Windows.Clou @{Microsoft.Windows.Clou @{Microsoft.Windows.Cort @{icrosoft.Windows.Cort @icrosoft.Windows.Cort	Domai Domai Domai Domai	Yes Yes Yes Yes Yes	Allow Allow Allow Allow	Disable Rule Cut Cut Copy Delete
	@ @FirewallAPI.dll,-80206 @FirewallAPI.dll,-80206 iTunes iTunes iTunes iTunes iTunes iTunes iTunes iTunes	©FirewallAPLdll-80200 @FirewallAPLdll-80200 (78E1CD88-49E3-476E-B926 (78E1CD88-49E3-476E-B926 (78E1CD88-49E3-476E-B926 (78E1CD88-49E3-476E-B926 (78E1CD88-49E3-476E-B926 (78E1CD88-49E3-476E-B926)	All All All All All All All	Yes Yes Yes Yes Yes Yes	Allow Allow Allow Allow Allow Allow	 Properties Help
	V iTunes ITunes	{78E1CD88-49E3-476E-B926 {78E1CD88-49E3-476E-B926	All	Yes	Allow	

4. Select "Custom" and then click "Next"

🔗 New Inbound Rule Wizard	4	×
Rule Type		
Select the type of firewall rule to o	reate.	
Steps: Program Protocol and Ports Scope Action Profile Name	What type of rule would you like to create? Program Rule that controls connections for a program. Predefined: @ Freedefined: @ Freedefined: We that controls connections for a Windows experience. @ Custom Custom rule.	
	< Back Next > Cancel	

5. Select "All programs" and then click "Next"

🔗 New Inbound Rule Wizard		×
Program		
Specify the full program path and exe	cutable name of the program that this rule matches.	
Steps:		
Rule Type	Does this rule apply to all programs or a specific program?	
Program		
Protocol and Ports	All programs	
Scope	Rule applies to all connections on the computer that match other rule properties.	
Action	○ This program path:	
Profile	Browse	
Name	Example: c:\path\program.exe %ProgramFiles%\browser\browser.exe	
	Services Customize Specify which services this rule applies to.	
	< Back Next > Cancel	

- 6. Select "Protocol Type:ICMPv4" and then click "customize" a new popup will appear.
 - a. Select "Specific ICMP Types" and then "Eco Request"b. Click 'OK" and then click "Next"

			Customize ICMP Settings	×			
Specify the protocols and ports to v	which this rule applies.		Apply this rule to the following Internet Control Message Protocol (ICMP) connections:				
Steps:			O All ICMP types				
Rule Type	To which ports and p	protocols does this rule apply?	Specific ICMP types	_			
Program			Destination Unreachable				
Protocol and Ports	Protocol type:	ICMPv4 ~	Source Quench				
Scope	Protocol number:	1	Echo Request	1			
Action							
Profile Name	Local port:	All Ports ~	Time Exceeded Parameter Problem				
• Name		Example: 80 443 5000-5010	Timestamp Request				
	Remote port:	All Ports					
		Example: 80, 443, 5000-5010					
	Internet Control Mes	sage Protocol Customize					
	(ICMP) settings:		This ICMP type:				
			Type: 0 ~ Code: Any ~ Add				
			OK Cance	el			
		< Back	Next > Cancel				

7. Select "Any IP address" for both and then click "Next"

Scope	
Specify the local and remote IP ad	ddresses to which this rule applies.
Steps:	
a Rule Type	
Program	Which local IP addresses does this rule apply to?
Protocol and Ports	Any IP address
Scope	O These IP addresses:
Action	Add
Profile	Edit
Name	Remove
	Customize the interface types to which this rule applies: Customize
	Which remote IP addresses does this rule apply to? Any IP address These IP addresses:
	Add
	Eda
	Remove
	< Back Next > Cancel

8. The Action screen appears. Select "Allow the connection" and then click on "Next" button.



9. The Profile screen appears, make sure "Domain", "Private" and "public" should be selected and then click on "Next" button.



10. The Name screen appears. Enter a name and description for the rule (like ICMP Echo). Click "**Finish**". The rule will be added.

10	🕐 New Inbound Rule Wizard	3	×
N	lame		
Sp	becify the name and description	of this rule.	
s	leps:		
۲	Rule Type		
۲	Program		
۲	Protocol and Ports		
۲	Scope	Name:	
۲	Action	ICMIP - Echo	
۲	Profile	Description (optional):	
۲	Name	enabling Ping to this Windows PC	
		< Back Finish Ca	ancel