Add Firewall Exception for SQL

Last Modified on 10/01/2015 2:22 am EDT

- 1. Click Start and type Firewall to find the Firewall application.
- 2. Click on the Windows Firewall application to launch it.
- 3. Click on Advanced Settings.



4. Click on Inbound Rules.

ile Action View Help						
			_	_	_	
Windows Firewall with Advance Windows Rules	Inbound Rules		_	_	_	Actions
Cutbound Rules	Name	Group	Profile	Enabled	Action ^	Inbound Rules
Connection Security Rules	VMware Authd Service		Domain	Yes	Allow	🙇 New Rule
	SVMware Authd Service (private)		Private	Yes	Allow	Filter by Profile
	VMware Workstation Server		Domain	Yes	Allow	
	W Wware Workstation Server (private)		Private	Yes	Allow	Filter by State
	BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr	All	No	Allow	Filter by Group
	BranchCache Hosted Cache Server (HTT	BranchCache - Hosted Cach	All	No	Allow	View
	BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove	All	No	Allow	
	CheckPoint.VPN	CheckPoint.VPN	All	Yes	Allow	Refresh
	Connect to a Network Projector (TCP-In)	Connect to a Network Proje	Private	No	Allow	is Export List
	Connect to a Network Projector (TCP-In)	Connect to a Network Proje	Domain	No	Allow	Help
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Domain	No	Allow	-
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Private	No	Allow	
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Private	No	Allow	
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Domain	No	Allow	
	Connect to a Network Projector (WSD-In)	Connect to a Network Proje	All	No	Allow	
	Core Networking - Destination Unreacha	Core Networking	All	Yes	Allow	
	Core Networking - Destination Unreacha	Core Networking	All	Yes	Allow	
	Core Networking - Dynamic Host Config	Core Networking	All	Yes	Allow	¥
	Core Networking - Dynamic Host Config	Core Networking	All	Yes	Allow	
	Core Networking - Internet Group Mana	Core Networking	All	Yes	Allow	
	Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	Allow	
	Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	Allow	
	Core Networking - Multicast Listener Do	Core Networking	All	Yes	Allow	
	Core Networking - Multicast Listener Qu	Core Networking	All	Yes	Allow	
	Core Networking - Multicast Listener Rep		All	Yes	Allow	
	Core Networking - Multicast Listener Rep		All	Yes	Allow	
	Core Networking - Neighbor Discovery A		All	Yes	Allow	
	Core Networking - Neighbor Discovery S		All	Yes	Allow	
	Core Networking - Packet Too Big (ICMP		All	Ves	Allow Y	
· >	< .				>	

5. Click New Rule.

e Action View Help	1.0	ewall with Advanced Secu				
+ 2 🖸 🕞 🛙 🗂						
Windows Firewall with Advance	Inbound Rules					Actions
Windows Firewall with Advance	Name VMware Authd Service VMware Authd Service (private) VMware Workstation Server VMware Workstation Server (private) BranchCache Content Retrieval (HTTP-In) BranchCache Hosted Cache Server (HTT BranchCache Peer Discovery (WSD-In) CheckPoint.VPN Connect to a Network Projector (TCP-In) Connect to a Network Projector (WSD Ev	Connect to a Network Proje Connect to a Network Proje Connect to a Network Proje Core Networking Core Networking Core Networking Core Networking Core Networking Core Networking Core Networking Core Networking Core Networking Core Networking	Domain Private Domain Private All All All Private Domain Domain Private Domain Private All All All All All All All All All	Enabled Yes Yes No No No No No No No No No No No No No	Action Allow	Actions Inbound Rules New Rule Filter by Profile Filter by State Filter by Group View Ca Refresh Filter by Help
>	Core Networking - Neighbor Discovery A Core Networking - Neighbor Discovery S Core Networking - Parket Ton Big (ICMP	Core Networking		Yes Yes Yes	Allow Allow Allow	

NIC

6. Choose to create a Port rule.



7. Enter port 1433 in the Specific local ports field. Click Next.



a	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	• TCP					
 Action 	○ UDP					
 Profile 						
Name	Does this rule apply to all local ports or specific local ports?					
	All local ports	×.				
	Specific local ports:	1433				
		ts or specific local ports?				
		Bas				
		.dos				
	and the	< Back Next > Cancel				

8. The action will be to "Allow the Connection" which is the default. Click Next.





9. Uncheck the Public profile. Click Next.



Profile Specify the profiles for which this rule applies. Steps: Protocol and Ports Action Protocol and Ports	
Rule Type When does this Protocol and Ports	
Applies who	a a computer is connected to its comparis domain
Name Name Private Applies whe or work plac Debuild	n a computer is connected to a private network location, such as a home e. n a computer is connected to a public network location.

10. Set the Name for this rule and click Finish.



@	New Inbound Rule Wizard	×
Name		
Specify the name and description of	of this rule.	
Steps:		
Rule Type		
 Protocol and Ports Action 		
Profile	Name:	
Name	SQL Firewall	
	Description (optional):	
	SQL Firewall Description (optional): Contituent Contituent Back Finish Cancel	
	C OIL	
	S	
	Bar	
	200	
	< Back Finish Cancel	

11. Close the Firewall panel by clicking X in the top-right corner.

RELATED ARTICLES [template("related")]