## **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.

Windows Firewall with Advanced Security					
File Action View Help					
🗢 🔿 🙇 🔂 🔂 🔂					
P Windows Firewall with Advance	Inbound Rules				Actions
	Inbound Rules Name VMware Authd Service VMware Authd Service VMware Authd Service (private) VMware Authd Service (private) VMware Workstation Server VMware Workstation Server (private) BranchCache Hosted Cache Server (HTT BranchCache Hosted Cache Server (HTT CheckPoint.VPN Connect to a Network Projector (TCP-In) Connect to a Network Projector (WSD Ev Connect to a Network Projector (WSD In) Core Networking - Destination Unreacha Core Networking - Dynamic Host Config Core Networking - Internet Group Mana Core Networking - IPHTTPS (TCP-In) Core Networking - IPHTTPS (TCP-In) Core Networking - IPHTTPS (TCP-In) Core Networking - Multicatt Littener Do	Group BranchCache - Content Retr BranchCache - Hosted Cach BranchCache - Hosted Cach BranchCache - Peer Discove CheckPoint.VPN Connect to a Network Proje Connect to a Network Proje Core Networking Core Networking Core Networking Core Networking Core Networking	Profile En. Domain Yee Private Yee All No All No All No All No All No Domain No Domain No Domain No Domain No All Yee All Yee All Yee All Yee All Yee All Yee	abled Action s Allow s Allow s Allow s Allow s Allow b Allow	Actions Inbound Rules New Rule Filter by Profile Filter by State Filter by Group View Refresh Export List Help
	Core Networking - Multicast Listener Qu Core Networking - Multicast Listener Rep	Core Networking Core Networking	All Ye	s Allow s Allow	
	Core Networking - Multicast Listener Rep Core Networking - Neighbor Discovery A Core Networking - Neighbor Discovery S Core Networking - Parket Top Big (ICMP	Core Networking Core Networking Core Networking	All Ye All Ye All Ye All Ye	s Allow s Allow s Allow s Allow	

NIC

## 5. Click New Rule.

<b>a</b>	Windows Firewall with Advanced Security - 🗖					= 🗆 ×
File Action View Help	.1.					
Windows Firewall with Advance	Inbound Rules		_	_		Actions
K Inbound Rules	Name	Course A	Deafile	Easthlad /	ation A	Jahound Pulos
Cutbound Rules	Name	Group	Profile 1	Enabled A	Action	Inbound Rules
Security Rules	VMware Autho Service		Domain	Yes /	Allow	New Rule
Monitoring	WMware Autho Service (private)		Private	Yes A	Allow	🐨 Filter by Profile 🕨 🕨
	VMware Workstation Server		Domain	Yes A	Allow	🐨 Filter by State 🕨
	Visiware workstation Server (private)     Provide Content Patricial (UTTD In)	Procedure Contract Pate	All	Ne /	Allow	V Filter by Group
	Prosth Cache Content Retheval (HTT	BranchCache - Content Ketr		No A	Allow	· merey or op
	BranchCache Plosted Cache Server (H111	BranchCache - Plosted Cach		No /	Allow	View
	CharkBoint VDN	CharleDoint VDN		Ver /	Mow	G Refresh
	Connect to a Network Projector (TCP-In)	Connect to a Network Proje	Private I	No /	llow	Export List
~` <b>O</b>	Connect to a Network Projector (TCP-In)	Connect to a Network Proje	Domain I	No /	llow	
	Connect to a Network Projector (WSD Ev-	Connect to a Network Proje	Domain I	No /	Allow	E nep
	Connect to a Network Projector (WSD Ev-	Connect to a Network Proje	Private	No 4	Allow	
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Private	No 4	Allow	
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Domain I	No 4	Allow	1
	Connect to a Network Projector (WSD-In)	Connect to a Network Proje	All I	No 4	Allow	
	Core Networking - Destination Unreacha	Core Networking	All	Yes 4	Allow	1
	Core Networking - Destination Unreacha	Core Networking	All 1	Yes 4	Allow	1
	Core Networking - Dynamic Host Config	Core Networking	All I	Yes /	Allow	1
	Core Networking - Dynamic Host Config	Core Networking	All I	Yes A	Allow	1
	Ocore Networking - Internet Group Mana	Core Networking	All 1	Yes A	Allow	
	Core Networking - IPHTTPS (TCP-In)	Core Networking	All 1	Yes 4	Allow	
	Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes 4	Allow	
	Ocore Networking - Multicast Listener Do	Core Networking	All 1	Yes /	Allow	1
	Core Networking - Multicast Listener Qu	Core Networking	All 1	Yes 4	Allow	1
	Core Networking - Multicast Listener Rep	Core Networking	All 1	Yes A	Allow	1
	Core Networking - Multicast Listener Rep	Core Networking	All	Yes A	Allow	1
	Core Networking - Neighbor Discovery A	Core Networking	All	Yes A	Allow	
	Core Networking - Neighbor Discovery S	Core Networking	All	Yes 4	Allow	
(	Core Networking - Parket Too Rig (ICMP	Core Networking	All	Ves 1	Allow Y	
,					-	

6. Choose to create a Port rule.



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



<b>a</b>	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			
<ul> <li>Action</li> </ul>				
<ul> <li>Profile</li> </ul>				
<ul> <li>Name</li> </ul>	Does this rule apply to all local ports or specific local ports?			
	O All local ports			
	Specific local ports:	1433		
		Example: 80, 443, 5000-5010		
		Base		
		200 <sup>e</sup>		
	- SN'	< 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.



<b>@</b>	New Inbound Rule Wizard			
Profile Specify the profiles for which this	s rule applies.			
Steps: Protocol and Ports Action	When does this rule apply?   Domain			
<ul> <li>Profile</li> <li>Name</li> </ul>	Applies when a computer is connected to its corporate domain.  Physic  Applies when a computer is connected to a private network location, such as a home or work place.  Public  Applies when a computer is connected to a public network location.  Applies when a computer is connected to a public network location.  Confit to the computer is connected to a public network location.  Confit to the computer is connected to a public network location.  Confit to the computer is connected to a public network location.  Confit to the computer is connected to a public network location.  Confit to the computer is connected to a public network location.  Confit to the computer is connected to a public network location.  Confit to the computer is connected to a public network location.  Confit to the computer is connected to a public network location.  Confit to the computer is connected to a public network location.  Confit to the computer is connected to a public network location.  Confit to the computer is connected to a public network location.  Confit to the computer is connected to a public network location.  Confit to the computer is connected to a public network location.  Confit to the computer is connected to a public network location.  Confit to the computer is connected to a public network location.  Confit to the computer is connected to a public network location.  Confit to the computer is connected to a public network location.  Confit to the computer is connected to a public network location.  Confit to the computer is connected to a public network location.  Confit to the computer is connected to a public network location.  Confit to the computer is connected to a public network location.  Confit to the computer is connected to a public network location.  Confit to the computer is connected to a public network location.  Confit to the computer is connected to a public network location.  Confit to the computer is connected t			

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



<b>@</b>	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):	
	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")]