

# **Check Blocked IPs**

1. Right click on the windows logo on the left bottom corner, after then left click on the Run

Power Options Event Viewer System Device Manager Network Connections Disk Management Computer Management Computer Management Command Prompt Command Prompt (Admin) Task Manager Control Panel File Explorer Search	Programs and Features
Event Viewer System Device Manager Network Connections Disk Management Computer Management Command Prompt Command Prompt (Admin) Task Manager Control Panel File Explorer Search Run	Power Options
System Device Manager Network Connections Disk Management Computer Management Command Prompt Command Prompt (Admin) Task Manager Control Panel File Explorer Search	Event Viewer
Device Manager Network Connections Disk Management Computer Management Command Prompt Command Prompt (Admin) Task Manager Control Panel File Explorer Search	System
Network Connections Disk Management Computer Management Command Prompt Command Prompt (Admin) Task Manager Control Panel File Explorer Search	Device Manager
Disk Management Computer Management Command Prompt Command Prompt (Admin) Task Manager Control Panel File Explorer Search Run	Network Connections
Computer Management Command Prompt Command Prompt (Admin) Task Manager Control Panel File Explorer Search Run	Disk Management
Command Prompt Command Prompt (Admin) Task Manager Control Panel File Explorer Search Run	Computer Management
Command Prompt (Admin) Task Manager Control Panel File Explorer Search Run	Command Prompt
Task Manager Control Panel File Explorer Search Run	Command Prompt (Admin)
Control Panel File Explorer Search Run	Task Manager
File Explorer Search Run	Control Panel
Search V	File Explorer 🚽 🖕
Run	Search
	Run
Shut down or sign out	Shut down or sign out
Desktop	Desktop

2. Type wf.msc, then press Enter

	Run 🛛 🗶
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	<mark>₩f.msc</mark> ✓ This task will be created with administrative privileges.
	OK Cancel <u>B</u> rowse

### 3. Click on inbound rules

irevall with Advance	Inbound Rules											Actions
d Rules	Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Pc	Inbound Rules
Connection Security Rules Monitoring	SrdpProtect block: 37.76.114.2		All	Ves	Block	No	Arry	Any	37.76.114.2	Any	Any	1 New Rule
	Ordpguard-7218b319-local	RdpGuard	All	No	Block	No	Any	Any	185.132.250.5	Any	Any	
	World Wide Web Services (HTTPS Traffic	Secure World Wide Web Ser	All	Yes	Allow	No	System	Any	Any	TCP	443	V Filter by Profile
	World Wide Web Services (HTTP Traffic-L	World Wide Web Services (	All	Yes	Allow	No	System	Any	Any	TCP	80	Tilter by State
	Windows Remote Management (HTTP-In)	Windows Remote Manage	Public	Yes	Allow	No	System	Any	Local subnet	TCP	5985	T Filter by Group
	Windows Remote Management (HTTP-In)	Windows Remote Manage	Domai_	Yes	Allow	No	System	Arry	Any	TCP	5985	View
	Windows Remote Management - Compa_	Windows Remote Manage	All	No	Allow	No	System	Any	Any	TCP	80	
	Windows Management Instrumentation	Windows Management Instr	All	No	Allow	No	%System	Any	Any	TCP	Any	Ci Refresh
	Windows Management Instrumentation	Windows Management Instr	All	No	Allow	No	%System	Any	Any	TCP	135	Export List
	Windows Management Instrumentation	Windows Management Instr	All	No	Allow	No	%system	Any	Any	TCP	Any	El bielo
	Windows Firewall Remote Management (	Windows Firewall Remote	All	No	Allow	No	%System	Arry	Any	TCP	RPC Ene	El rich
	Windows Firewall Remote Management (	Windows Firewall Remote	All	No	Allow	No	%System	Amy	Any	TCP	RPC Dye	rdpProtect block 37.76.114.
	Virtual Machine Monitoring (RPC)	Virtual Machine Monitoring	All	No	Allow	No	%System	Any	Any	TCP	RPC Dyi	Disable Rule
	Witual Machine Monitoring (NB-Session	Virtual Machine Monitoring	All	No	Allow	No	Any	Any	Any	TCP	139	N CA
	Virtual Machine Monitoring (Echo Reque	Virtual Machine Monitoring	All	No	Allow	No	Any	Arry	Any	ICMPv6	Any	A COL
	Wirtual Machine Monitoring (Echo Reque	Virtual Machine Monitoring	All	No	Allow	No	Any	Any	Any	ICMPv4	Any	山田 Copy
	Wirtual Machine Monitoring (DCOM-In)	Virtual Machine Monitoring	All	No.	Allow	No	%System	Any	Any	TCP	135	X Delete
	TOLL Vistual Court Card Management /T	TOM Vietual Conart Card Ma	Drivata	Min	Allena	bin	QCContarts.	Amu	Local rubnat	TCD	Am	



#### 4. Click on the Action column twice to see the blocked entries first

Advance	Inbound Rules											Actions
	Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Por A	Inbound Rules
	SetpProtect block: 37.76.114.2	SHARE WE	All	Ves	Block	No	Any	Any	37.76.114.2	Any	Any	New Rule
	Ordpguard-7218b319-local	RdpGuard	All	No	Block	No	Any	Any	185.132.250.5	Any	Any	Titler by Donfile
	World Wide Web Services (HTTPS Traffic	Secure World Wide Web Ser	All	Yes	Allow	No	System	Amy	Any	TCP	443	• File by Filme
	World Wide Web Services (HTTP Traffic-L.	World Wide Web Services (	All	Yes	Allow	No	System	Any	Any	TCP	80	Y Filter by State
Windows Remote Management	Windows Remote Management (HTTP-In)	Windows Remote Manage	Public	Yes	Allow	No	System	Any	Local subnet	TCP	5985 1	Filter by Group
	Windows Remote Management (HTTP-In)	Windows Remote Manage	Domai_	Yes	Altow	No	System	Any	Any	TCP	5985	View
	Windows Remote Management - Compa	Windows Remote Manage	All	No	Allow	No	System	Any	Any	TCP	80	2 Adust
	Windows Management Instrumentation	Windows Management Instr	All	No	Allow	No	%System	Amy	Any	TCP	Any	CA NETICAL
	Windows Management Instrumentation	Windows Management Instr	All	No	Allow	No	%System	Any	Any	TCP	135	Export List
	Windows Management Instrumentation	Windows Management Instr	AB	No	Allow	No	%system_	Any	Any	TCP	Any	Help
- 13	Windows Firewall Remote Management (	Windows Firewall Remote	All	No	Allow	No	%System	Amy	Any	TCP	RPC End	The second second second second
	Windows Firewall Remote Management (	Windows Firewall Remote	All	No	Allow	No	%System	Any	Any	TCP	RPC Dyn	rdpProtect block 37.76.114.2
	Virtual Machine Monitoring (RPC)	Virtual Machine Monitoring	All	No	Allow	No	%System	Any	Any	TCP	RPC Dyn	Disable Rule
	Virtual Machine Monitoring (NB-Session	Virtual Machine Monitoring	All	No	Allow	No	Any	Any	Arry	TCP	139	& Cut
- 1	Virtual Machine Monitoring (Echo Reque	Virtual Machine Monitoring	All	No	Allow	No	Any	Any	Any	ICMPv6	Any	R. Com
	Virtual Machine Monitoring (Echo Reque	Virtual Machine Monitoring	All	No	Allow	No	Any	Any	Any	ICMPv4	Any	dill copy
	Virtual Machine Monitoring (DCOM-In)	Virtual Machine Monitoring	All	No	Allow	No	%System	Amy	Any	TCP	135	× Delete
	IPM Virtual Smart Card Management (T	TPM Virtual Smart Card Ma	Private	No	Allow	No	%System	Any	Local subnet	TCP	Any	Fill Brenastian

## 5. Right click on a rule prefixed with rdpProtect block:

indows Firewall with Advance	Inbound Rules												Actions	
inbound Rules	Name	oroup	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Pr	^	Inbound Rules	
Connection Security Pulse	SidpProtect block: 37.76314.2										Any		New Rule	
inection security nules	Srdpguard-7218b319-local	RdpGuard	All	No	Block	No	Any	Any	185.132.250.5	Any	Any			
moning	World Wide Web Services (HTTPS Traffic	Secure World Wide Web Ser	All	Yes	Allow	No	System	Any	Any	TCP	443		Y Filter by Profile	
	World Wide Web Services (HTTP Traffic-I	World Wide Web Services (	All	Yes	Allow	No	System	Any	Any	TCP	80		Filter by State:	
	Windows Remote Management (HTTP-In)	Windows Remote Manage	Public	Yes	Allow	No	System	Any	Local subnet	TCP	5985	-	Y Filter by Group	
	Windows Remote Management (HTTP-In)	Windows Remote Manage	Domai_	Yes	Allow	No	System	Any	Any	TCP	5985	22	Mari	
	Windows Remote Management - Compa	Windows Remote Manage	All	No	Allow	No	System	Any	y Any TCP	TCP	80		vew .	
	Windows Management Instrumentation	Windows Management Instr	All	No	Allow	No	%System	Any	Any	TCP	Any		G Refresh	
	Windows Management Instrumentation	Windows Management Instr	All	No	Allow	No	%System	Any	Any	TCP	135		Export List	
	Windows Management Instrumentation	Windows Management Instr	All	No	Allow	No	%system	Any	Any	TCP	Any	- 17	E Mala	
	Windows Firewall Remote Management (	Windows Firewall Remote	All	No	Allow	No	%Sustem	Anv	Ame	TCP	RPC Fre	11	Help	

## 6. Right click on a rule prefixed with rdpProtect block:, and press Delete

Inbound Rules										
Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Pot A
SrdpProtect block: 37.76.114.2		All	Ver	Plack						Any
Srdpguard-7218b319-local	RdpGuard	All	Disable Rule		No	Any	Any	185.132.250.5	Any	Any
World Wide Web Services (HTTPS Traffic	Secure World Wide Web Ser	AII	Cut		No	System	Any	Any	TCP	443
World Wide Web Services (HTTP Traffic-I	World Wide Web Services (	All	Copy		No	System	Any	Any	TCP	80
Windows Remote Management (HTTP-In)	Windows Remote Manage	Pu	Delete		No	System	Any	Local subnet	TCP	5985 =
Windows Remote Management (HTTP-In)	Windows Remote Manage	Dc	Delete		No	System	Any	Any	TCP	5985
Windows Remote Management - Compa	Windows Remote Manage	AII	Properties		No	System	Any	Any	TCP	80
Windows Management Instrumentation	Windows Management Instr	All	Help		No	%System	Any	Any	TCP	Any
Windows Management Instrumentation	Windows Management Instr	All	IND	Allow	No	%System	Any	Any	TCP	135
Windows Management Instrumentation	Windows Management Instr	All	No	Allow	No	%system	Any	Any	TCP	Any
Windows Firewall Remote Management (	Windows Firewall Remote	All	No	Allow	No	%System	Any	Any	TCP	RPC End
Windows Firewall Remote Management (	Windows Firewall Remote	ΔII	No	Allow	No	%System	Δnv	Anv	TCP	RPC Dyn

### 7. Successfully deleted

ewall with Advance	Inbound Rules											Actions	
Rules	Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Pc ^	Inbound Rules	
Concurity Rules	Ordpguard-7218b319-local	RdpGuard	All	No	Block	No	Any	Any	185.132.250.5	Any	Any	1 New Rule	
runes.	World Wide Web Services (HTTPS Traffic	Secure World Wide Web Ser	All	Yes	Allow	No	System	Any	Any	TCP	443	ST Charles Ch	
	World Wide Web Services (HTTP Traffic-L.	World Wide Web Services (	All	Yes	Allow	No	System	Any	Any	TCP	80	Y Filter by Protile	
	Windows Remote Management (HTTP-In)	Windows Remote Manage	Public	Yes	Allow	No	System	Any	Local subnet	TCP	5985	Filter by State	
	Windows Remote Management (HTTP-In)	Windows Remote Manage	Domai	Yes	Allow	No	System	Any	Any	TCP	5985	Y Filter by Group	
	Windows Remote Management - Compa	Windows Remote Manage	All	No	Allow	No	System	Any	Any	TCP	80	View	
	Windows Management Instrumentation	Windows Management Instr	All	No	Allow	No	%System	Any	Any	TCP	Any	The second secon	
	Windows Management Instrumentation	Windows Management Instr	All	No	Allow	No	%System	Any	Any	TCP	135	G Refresh	
	Windows Management Instrumentation	Windows Management Instr	All	No	Allow	No	%system	Any	Any	TCP	Any	Export List	
	Windows Firewall Remote Management (	Windows Firewall Remote	All	No	Allow	No	%System	Any	Any	TCP	RPC Enr	Help	
	Windows Firewall Remote Management (	Windows Firewall Remote	All	No	Allow	No	%System	Any	Any	TCP	RPC Dyr	E	_
	Wirtual Machine Monitoring (RPC)	Virtual Machine Monitoring	All	No	Allow	No	%System	Any	Any	TCP	RPC Dyr	rdpguard-7218b319-local	
	Virtual Machine Monitoring (NB-Session	Virtual Machine Monitoring	All	No	Allow	No	Any	Any	Any	TCP	139	O Enable Rule	
	Wirtual Machine Monitoring (Echo Reque	Virtual Machine Monitoring	All	No	Allow	No	Any	Any	Any	ICMPv6	Any	K Ca	
	Wirtual Machine Monitoring (Echo Reque	Virtual Machine Monitoring	All	No	Allow	No	Any	Any	Any	ICMPv4	Any	a cu	
	Wirtual Machine Monitoring (DCOM-In)	Virtual Machine Monitoring	All	No	Allow	No	%System	Any	Any	TCP	135	Copy	
	TPM Virtual Smart Card Management (T-	TPM Virtual Smart Card Ma	Private_	No	Allow	No	%System	Any	Local subnet	TCP	Any	🔀 Delete	
	TPM Virtual Smart Card Management (T	TPM Virtual Smart Card Ma	Domain	No	Allow	No	%System	Any	Any	TCP	Any	Properties	
	TPM Virtual Smart Card Management (D	TPM Virtual Smart Card Ma	Domain	No	Allow	No	%System	Any	Any	TCP	135		
	TPM Virtual Smart Card Management (D_	TPM Virtual Smart Card Ma	Private_	No	Allow	No	%System	Any	Local subnet	TCP	135	Help	