WMDC + Windows Defender Firewall

Allowing 'Enable advanced network functionality' to work. This allows WMDC to work at high speed.





Click on 'Advanced settings'

Windows Defender Firewall with	h Advanced Security							-	×
File Action View Help									
Þ 🔿 🙍 📆 🗟 🚺									
P Windows Defender Firewall wit	Ji thound Rules					Acti	ons		 _
and incound fidics	Name	Group	Profile	Enable	•	0*	hound Pulse		
Outbound Rules	G @FirewellAPI.dll,-80204	@FirewallAPI.dll,-80200	ы 2		H	83	New Rule		
> 戅 Monitoring	AllJoyn Router (TCP-Out)	AllJoyn Router	Domai	Yes	ч	v	Filter by Profile		
	GAIJoyn Router (UDP-Out)	AllJoyn Router	Dorlai	Yes		-	Filter by State		
	BranchCache Content Retrieval (HTTP-O	BranchCache - Content Retr	All 🚩	No		÷.	The by state		
	BranchCache Hosted Cache Client (HTTP	BranchCache - Hosted Cach	All	No		1¥.	Filter by Group		
	BranchCache Hosted Cache Server(HTTP	BranchCache - Hosted Cach	All	No			View		
	BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discove	All	No		a	Refresh		
	Cast to Device functionality (qWave-TCP	Cast to Device functionality	Private	Yes			-		
	Cast to Device functionality (qWave-UDP	Cast to Device functionality	Private	Yes			Export List		
	Cast to Device streaming server (RTP-Stre	Cast to Device functionality	Private	Yes		?	Help		
	Cast to Device streaming server (RTP-Stre	Cast to Device functionality	Domain	Yes		-			
	Cast to Device streaming server (RTP-Stre	Cast to Device functionality	Public	Yes	×				
< > >	<			>					

Click on Outbound Rules, then click on 'New Rule...'

 Mew Outbound Rule Wizard Rule Type Select the type of firewall rule to create 	te.	×
Steps: Protocol and Ports Action Profile Name	What type of rule would you like to create? Program Rule that controls connections for a program. P Pg1 Rule that controls connections for a TCP or UDP port. Proglefined: @ FrewallAPI.dl, 80200 Rule that controls connections for a Windows experience. @ Qustom Custom rule.	

Click on Port, then Next

🔗 New Outbound Rule Wizar	d		×
Protocol and Ports			
Specify the protocols and ports to	which this rule applies.		
Steps: Protocol and Ports Action	Does this rule apply to TCP or UD	P?	
 Profile Name 	Does this rule apply to all remote p	orts or specific remote ports?	
	Specific remote ports:	5679 Example: 80, 443, 5000-5010	Next > Cancel

Select UDP; Specific remote port = 5679, then click on Next

💣 New Outbound Rule Wiza	rd	×
Action		
Specify the action to be taken whe	en a connection matches the conditions specified in the rule.	
Steps:		
Rule Type	What action should be taken when a connection matches the specified conditions?	
Protocol and Ports	Allow the connection	
Action	This includes connections that are protected with IPsec as well as those are not.	
Profile	Allow the connection if it is secure	
• Name	Anor the generation in it is sector This includes only connections that have been authenticated by using IPsec. Connection Security Custom The security is a sector of the security of the security Security Security Security	

Click on 'Allow the connection', then click Next

🔗 New Outbound Rule Wizar	d	\times
Profile		
Specify the profiles for which this n	ile applies.	
Steps:		
 Rule Type Protocol and Ports 	When does this rule apply?	
Action Profile	Domain Applies when a computer is connected to its corporate domain.	
Name	Private 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. (Back Next > Cancel	

Select all three domains, then click on Next

🔗 New Outbound Rule Wiza	ard	>
Name		
Specify the name and description	of this rule.	
Steps:		
Rule Type		
Protocol and Ports		
Action		
Profile	Name:	
Name	WMDC_Usen	
	Description (optional):	
	< <u>B</u> ack <u>F</u> inish	Cancel

Enter an appropriate name "WMDC_User" then click on Finish.

Next add a new Inbound Rule:

🔐 Windows Defender Firewall with	h Advanced Security							-	×
<u>File Action View H</u> elp									
Þ 🔿 🙍 📆 🗟 🚺									
windows berender Fire vall with	Inbound Rules					Ac	tions		
Inbound Rules	Name	Group	Profile	Enabl	e 🍾	Int	ound Rules		
So Connection Security Rules	Spotify.exe		Private	Yes	н	63	New Rule		
> 戅 Monitoring	Spotify.exe		Private	Yes	1	V	Filter by Profile		
	G @FirewallAPI.dll,-80201	@FirewallAPI.dll,-80200	All	Yes		7	Filter by State		
	Alliovo Router (TCP-In)	Alliovo Router	Domai	Ves		8	Filter by Group		
	AllJoyn Router (UDP-In)	AllJoyn Router	Domai	Yes		-	View		
	BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr	All	No			Defeet		
	BranchCache Hosted Cache Server (HTTP	BranchCache - Hosted Cach	All	No			Kerresh		
	BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove	All	No			Export List		
	Cast to Device functionality (qWave-TCP	Cast to Device functionality	Private	Yes		?	Help		
	Cast to Device functionality (qWave-UDP	Cast to Device functionality	Private	Yes					
	Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes	~				
< > >	<			2					

Click on Inbound Rules, then click on New Rule:

💣 New Inbound Rule Wiza	rd	×
Rule Type		
Select the type of firewall rule to	create.	
Steps:		
Rule Type	What type of rule would you like to create?	
Protocol and Ports		
Action	O <u>P</u> rogram	
Profile	Rule that controls connections for a program.	
Name	Port	
	Rule that controls connections for a TCP or UDP port.	
	O Predefined:	
	@FirewallAP1.dll,-80200	\sim
	Rule that controls connections for a Windows experience.	
	○ <u>C</u> ustom	
	Custom rule.	
	< Back Next >	Cancel

Click on 'Port', then click on Next

💣 New Inbound Rule Wiza	rd	
Protocol and Ports		
Specify the protocols and ports	to which this rule applies.	
Steps:		
Rule Type	Does this rule apply to TCP or U	DP?
Protocol and Ports	<u>Т</u> СР	
Action	() <u>U</u> DP	
Profile		
Name	Does this rule apply to all local p	orts or specific local ports?
	Specific local ports	990 999 5678 5679 5721 26675
	0	Example: 80, 443, 5000-5010
		< Back Next > Cancel

Select 'TCP'; enter these ports "990,999,5678,5679,5721,26675", click Next

🔗 New Inbound Rule Wiz	ard	×
Action		
Specify the action to be taken	when a connection matches the conditions specified in the rule.	
Steps:		
Rule Type	What action should be taken when a connection matches the specified conditions?	
Protocol and Ports	Allow the compation	
Action	This includes connections that are protected with IPsec as well as those are not	
Profile		
• Name	 Allow the gonnection if it is secure This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node. Customge Block the connection 	
	< <u>B</u> ack <u>N</u> ext > Cancel	

Click 'Allow the connection', click on Next

		```
www.inbound.Kule.wizard		
Profile		
Specify the profiles for which this n	ule applies.	
Stone -		
Rule Type	When does this rule apply?	
Protocol and Ports		
Action	✓ Domain	
Profile	Applies when a computer is connected to its corporate domain.	
Name	Private Applies when a computer is connected to a private network location, such as a home or work place.     Piplic Applies when a computer is connected to a public network location.	ncel

Select all three domains

💣 New Inbound Rule Wizar	d	×
Name		
Specify the name and description	i of this rule.	
Steps:		
Rule Type		
Protocol and Ports		
Action		
Profile	Name:	
Name	WMDC_User	
	Description (optional):	
	< <u>B</u> ack <u>F</u> inish	Cancel

Enter an appropriate name, then click 'Finish'

Unplug your T18, then plug it back in again. WMDC should connect in high speed NRDIS mode.