

WMDC + Windows Defender Firewall: RNDIS

Date: 9 December, 2019

By: Mark Silver, ms@igage.com

D:\GoogleDrive\Masters\Howay\T18\RNDIS\WMDC_RNDIS_008.docx

Thesis

If you have watched my video (<u>https://youtu.be/VHI4dwVbGbI</u>) and read the accompanying document (<u>http://igage.com/v/bin/WMDC_Win10_CreatorsEdition_Fix_RevB.pdf</u>) then you should have some idea that WMDC is disabled by default in Windows 10 and you have to 'do some stuff' to make it work again.

One of the steps in my list of 'stuff' is to uncheck the box 'Enable advanced network functionality':



Enable advanced network functionality



When you uncheck the box, instead of using RNDIS the connection is made by a virtual serial port service.

RNDIS is an embedded USB RNDIS host class driver provides a virtual Ethernet link over USB. Remote Network Driver Interface Standard (RNDIS) is a Microsoft proprietary protocol.

Unchecking the box is easy and results in a working system most of the time.

However, checking the box makes data transfers MUCH more reliable and over 3 times faster in most instances.

The problem with checking the box is most firewalls actively block WMDC.

This document shows how to edit the Windows Defender Firewall to allow WMDC to work.

Getting Started

Disconnect your data collector from your computer. Check the 'Enable advanced network functionality' check box:

Enable advanced network functionality



Plug your data collector into your computer. Wait a while for the network driver to be installed, you can watch for it in Device Manager under 'Network Adapters':



If you are not running a firewall or if your firewall already has an exclusion for WMDC then you will be able to start WMDC and see a connection:



If it can be started, you are done. No need for the rest of this document.

Verify that the problem is your Firewall

In preparation for briefly turning off your firewall, remove your computer from the internet by disconnecting the Ethernet cable and turning off Wi-Fi.

Turn off the firewall. In 'Windows Defender' this can be done by finding the active network:



Click on the active network (the blue text):





Turn off the Firewall.

Plug your data collector in and start WMDC on your computer desktop. If WMDC starts and connects, then your firewall is the problem. Continue with the rest of this document. If WMDC does not connect, then there is another issue beyond the scope of this document.

In either case, turn the firewall back on and connect your computer to the internet again.

Adding Exclusions to Windows Defender for WMDC

From the 'Firewall & network protection menu'



Click on 'Advanced settings'





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

🔗 New Outbound Rule V	Wizard	×
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 Program	
 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	
	Rule that controls connections for a Windows experience.	
	○ <u>C</u> ustom	
	Custom rule.	
	< <u>B</u> ack <u>N</u> ext > Cancel	

Click on Port, then Next

		~
W New Outbound Rule Wi	izard	~
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	○ ĪCP	
Action	UDP	
Profile		
Name	Does this rule apply to all remote ports or specific remote ports?	
	Specific remote ports 5679	
	Example: 80, 443, 5000-5010	
	< <u>B</u> ack <u>N</u> ext > Cancel	1

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



Click on 'Allow the connection', then click Next

💣 New Outbound Rule W	zard	×
Profile		
Specify the profiles for which th	is rule applies.	
Steps:		
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. Public Applies when a computer is connected to a public network location. 	
	< <u>B</u> ack <u>N</u> ext > Cancel	

Select all three domains, then click on Next

5



💣 New Outbound Rule Wiz	ard	×
Name		
Specify the name and description	n of this rule.	
Steps:		
Rule Type		
Protocol and Ports		
Action		
Profile	Name:	
Name	WMDC_User	
	Description (optional):	
	Canool Finish Canool	

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

Next add a new Inbound Rule:

Windows Defender Firewall with	Advanced Security						-	×
<u>File</u> <u>Action</u> <u>View</u> <u>H</u> elp								
🗢 🤿 🙋 📷 🗟 🚺 📷								
windows Derender Fire vall with	Inbound Rules					Actions		
Cuthound Rules	Name	Group	Profile	Enable	-	Inhound Rules		
L Connection Security Rules	🛇 spotify.exe		Private	Yes		🗱 New Rule		
> 🖳 Monitoring	S spotify.exe		Private	Yes	1	Filter by Profile		
	@FirewallAPI.dll,-80201	@FirewallAPI.dll,-80200	All	Yes		Filter by State		
	@FirewallAPI.dll,-80206	@FirewallAPI.dll,-80200	All	Yes				
	🔇 AllJoyn Router (TCP-In)	AllJoyn Router	Domai	Yes		Filter by Group		1
	🔮 AllJoyn Router (UDP-In)	AllJoyn Router	Domai	Yes		View		1
	BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr	All	No		Refrerb		
	BranchCache Hosted Cache Server (HTTP	BranchCache - Hosted Cach	All	No		inche		
	BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove	All	No		Export List		
	🔇 Cast to Device functionality (qWave-TCP	Cast to Device functionality	Private	Yes		P Help		
	Sector 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	¥			
< >	<			>				

Click on Inbound Rules, then click on New Rule:



Click on 'Port', then click on Next

🔗 New Inbound Rule Wizard	ł		\times
Protocol and Ports			
Specify the protocols and ports to	which this rule applies.		
Steps:			
Rule Type	Does this rule apply to TCP or UI	OP?	
Protocol and Ports	<u>Т</u> СР		
Action	() <u>U</u> DP		
Profile			
Name	Does this rule apply to all local po	orts or specific local ports?	
	<u>All local ports</u>		
	Specific local ports:	990,999,5678,5679,5721,26675	
		Example: 80, 443, 5000-5010	
		(Barly Next) Consel	
		< Back Next > Cancel	

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

7



Click 'Allow the connection', click on Next

💣 New Inbound Rule Wiza	ard	\times
Profile		
Specify the profiles for which th	is rule applies.	
Steps:		
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. Public Applies when a computer is connected to a public network location. 	
	< Back Next > Cancel	

Select all three domains

8





Namo		
Name		
specily the name and description	or this rule.	
Steps:		
Rule Type		
Protocol and Ports		
Action		
Profile	Name:	
Name	WMDC_User	
	Description (optional):	

Enter an appropriate name, then click 'Finish'

Unplug your data collector, wait 20 seconds and then plug it back in again. Start WMDC.

WMDC should connect in high speed NRDIS mode.