

IDT technical Note: 0004 (2012/12/28)

"How to: allow the IDT Software to communicate through the Windows Firewall"

All the cameras that support gigabit Ethernet communication may have issues if the Windows Firewall is installed. They communicate through the UDP network protocol and need to open ports to listen or receive images.

In most of the cases, the windows firewall shouldn't be disabled, the IDT software should be added to the list of the allowed programs and some firewall parameters should be configured (especially with HG cameras).

How to add IDT software to the list of allowed programs

When an Ethernet camera is operated for the first time, the Windows firewall detects the attempt to communicate through the network and tries to block it. The message below appears

Windows Secu	rity Alert	
💮 Windo	ows Firewal	l has blocked some features of this program
Windows Firewall h networks.	as blocked som	e features of Motion Inspector on all public and private
	<u>N</u> ame:	Motion Inspector
	Publisher:	IDT, Inc.
	Pat <u>h</u> :	C:\program files\idt\motioninspector\motioninspector.exe
Allow Motion Inspe	ctor to commun	icate on these networks:
✓ Private netw	vorks, such as m	iy home or work network
Public network because the	orks, such as the se networks off	ose in airports and coffee shops (not recommended ten have little or no security)
What are the risks	of allowing a pr	ogram through a firewall?
		Allow access Cancel

The software will be allowed to communicate through the network if both the private and public options are selected. Then click the "Allow access" button.

If the User Account Control (UAC) is disabled or you don't check both the options, you may still allow the communication through the firewall.

- From the control panel, start the Windows Firewall and select "Allow a program or feature through Windows Firewall".
- Scroll the list and make sure that "Motion Studio" is in and all the check boxes are selected (see below).



		- 0 X
🚱 🕞 🗢 🔐 « Win 🕨 Allowed 🔹 🍫 Se	arch Control Panel	٩
Allow programs to communicate through Wir To add, change, or remove allowed programs and ports, clic What are the risks of allowing a program to communicate?	ndows Firewall k Change settings.	nge settings
Allowed programs and features:	11 04/ L/D · · · >	
Name	Home/Work (Private)	Public
☐ iSCSI Service		
Media Center Extenders		
Motion Inspector		
Motion Studio - Image Acquisition and Processing		
□ Netlogon Service		
✓ Network Discovery		
Performance Logs and Alerts		
✓ readouttest.exe		
✓ Remote Assistance		
Remote Desktop		
Remote Desktop - RemoteFX		
Remote Event Log Management		
	Detai <u>l</u> s	Re <u>m</u> ove
	Allow anothe	r p <u>r</u> ogram
	ОК	Cancel



How to allow incoming echo requests (HG cameras)

HG cameras support the ICMP (Internet Control message Protocol). The cameras send a "ping" to the connected computer to check if the communication is still available. If the firewall blocks such packets the communication between the camera and the computer fails. For this reason, adding Motion Studio to the list of allowed programs is not enough.

In addition, ICMP echo requests should be allowed.

Windows XP

To detect if ICMP echo requests are allowed, open the Windows firewall and select the "Advanced Tab"

🗑 Windows Firewall 🛛 🛛 🔀	ICMP Settings
General Exceptions Advanced Network Connection Settings Windows Firewall is enabled for the connections selected below. To add exceptions for an individual connection, select it, and then click Settings: Image: Connection Settings Image: Connection 2 Settings Security Logging You can create a log file for troubleshooting purposes.	Internet Control Message Protocol (ICMP) allows the computers on a network to share error and status information. Select the requests for information from the Internet that this computer will respond to: Allow incoming echo request Allow incoming mask request Allow incoming router request Allow outgoing destination unreachable Allow outgoing source quench Allow outgoing parameter problem Allow outgoing ime exceeded Allow outgoing time exceeded Allow outgoing time exceeded
ICMP With Internet Control Message Protocol (ICMP), the computers on a network can share error and status information. Default Settings To restore all Windows Firewall settings to a default state, Restore Defaults Click Restore Defaults.	Allow outgoing packet too big Description Messages sent to this computer will be repeated back to the sender. This is commonly used for troubleshooting-for example, to ping a machine. Requests of this type are automatically allowed if TCP port 445 is enabled. OK Cancel

Click the ICMP settings and make sure that the "Allow incoming echo requests" option is selected.



Windows Vista / 7 / 8

- From the control panel, open the Windows Firewall and select the "Advanced settings" option (left pane). On Windows 8, the control panel can be open from the Metro start screen.
- Select the "Inbound rules" item on the left pane and find the following rules in the list:
 - 1. Windows Vista: "Networking Echo Request (ICMPv4-In)".
 - 2. Windows 7 and 8: "File and Printer sharing (Echo request ICMPv4-In)".
- If they are disabled (gray), select them and click the Enable rule button on the right pane or right click on the rule and select the "Enable rule" menu item (see below).

Inbound Rules				
Name	Group	Profile	Enab	*
File and Printer Sharing (Spooler Service	File and Printer Sharing	Domain	No	
Networking - Echo Request (ICMPv4-In)	Eile and Drinter Charine	Public	No	
Networking - Echo Request (ICMPv6-In)	Enable Rule	Public	No	
SCSI Service (TCP-In)	Delete	Private	No	
ISCSI Service (TCP-In)	Delete	Domain	No	
Media Center Extenders (HTTP-Streamin	Properties	Domai	No	
Media Center Extenders (qWave-TCP-In)	Usla	Domai	No	
Media Center Extenders (qWave-UDP-In)	пер	Domai	No	
Media Center Extenders (RDP-In)	Media Center Extenders	Domai	No	

Inbound Rules				
Name	Group	Profile	Enab	*
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction	Domain	No	
File and Printer Sharing (Echo Request - ICMPv4-In)	Enable Rule	Public	No	
🖉 File and Printer Sharing (Echo Request - ICMPv4-In)	Lindole Kule	Private	Yes	
🕑 File and Printer Sharing (Echo Request - ICMPv4-In)	Cut	Domain	Yes	
File and Printer Sharing (Echo Request - ICMPv6-In)	Сору	Public	No	
File and Printer Sharing (Echo Request - ICMPv6-In)	Delete	Domain	No	
🕑 File and Printer Sharing (Echo Request - ICMPv6-In)		Private	Yes	
🕑 File and Printer Sharing (LLMNR-UDP-In)	Properties	Private	Yes	
File and Printer Sharing (LLMNR-UDP-In)	Halp	Domain	No	
🕑 File and Printer Sharing (NB-Datagram-In)	Theip	Private	Yes	
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Public	No	





How to disable Windows firewall

To disable the Windows firewall the user needs Administrative privileges. The firewall separately manages three profiles and it should be disabled on all of them:

- Domain profile.
- Private Profile.
- Public Profile.

To disable the firewall, follow the instructions below

From the Control Panel, open the Windows Firewall dialog box.



From the options list on the left, select "Advanced Settings" and open the "Windows Firewall and advanced security" window.





Click the "Windows Firewall Properties" button and open the "Properties" dialog box.

Select the "Domain Profile" tab and set the "Firewall State" to off, then select the "Private Profile" and set the "Firewall State" to off, and then select the "Public Profile" and set the "Firewall State" to off.

omain Profile Private Profile Public	Profile IPsec Settings	
Specify behavior for when a comput domain. State	er is connected to its corp	orate
<u>Fi</u> rewall state:	Off	•
Inbound connections:	Block (default)	-
Outbound connection	s: Allow (default)	-
Protected network cor	nnections: Cu <u>s</u> tor	nize
Settings Specify settings that cont Firewall behavior.	rol Windows	mize
Logging Specify logging settings for troubleshooting.	or C <u>u</u> stor	nize
Logging Specify logging settings for troubleshooting.	or <u>Cu</u> stor	nize