



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

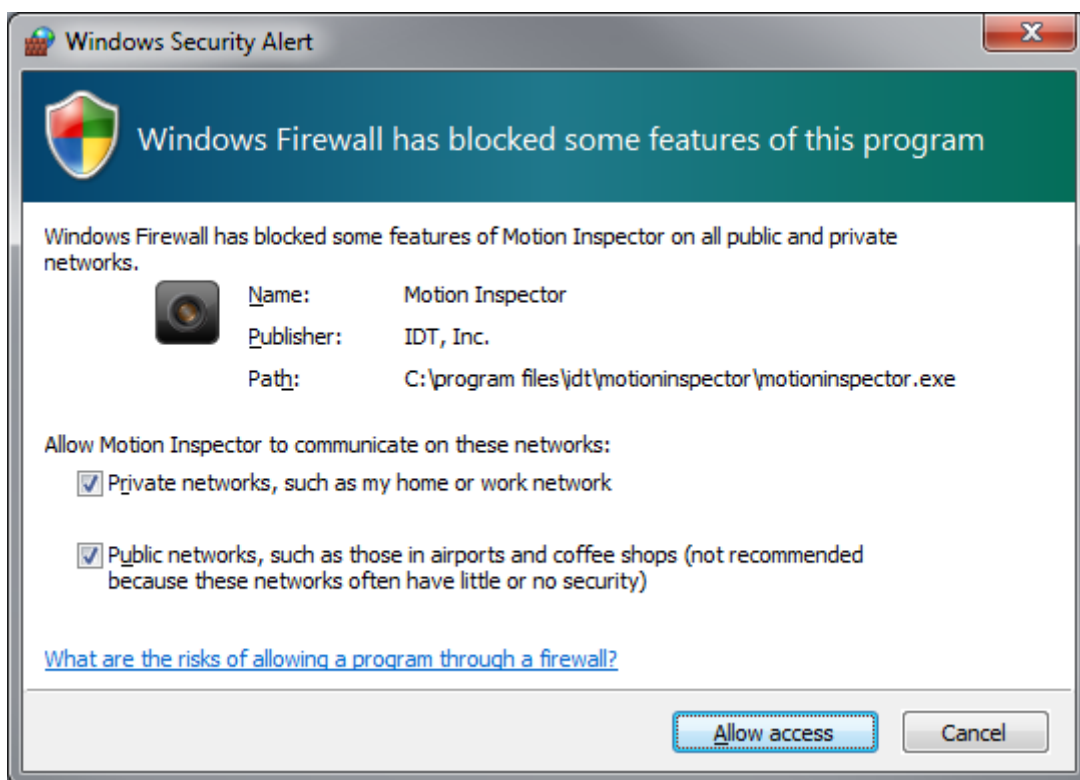
“How to: allow the IDT Software to communicate through the Windows Firewall”

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

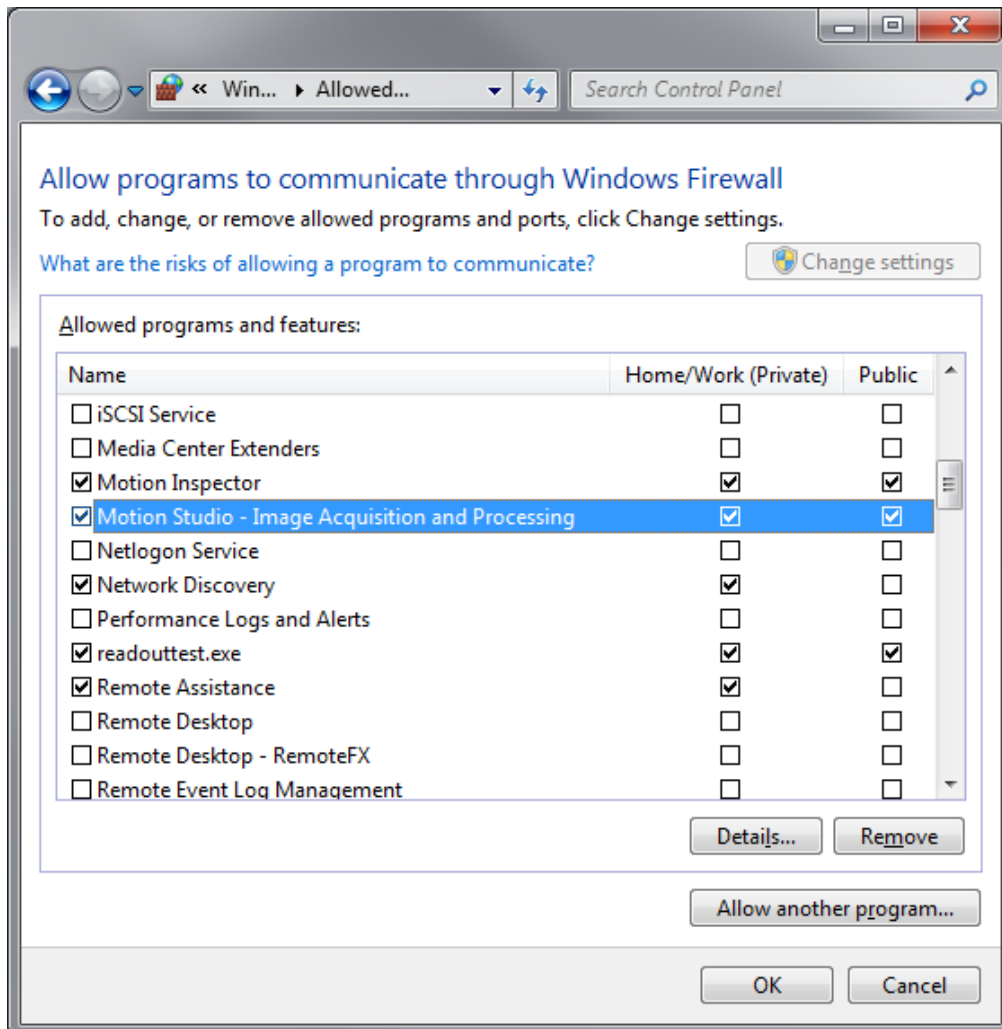
When an Ethernet camera is operated for the first time, the Windows firewall detects the attempt to communicate through the network and tries to block it. The message below appears



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).





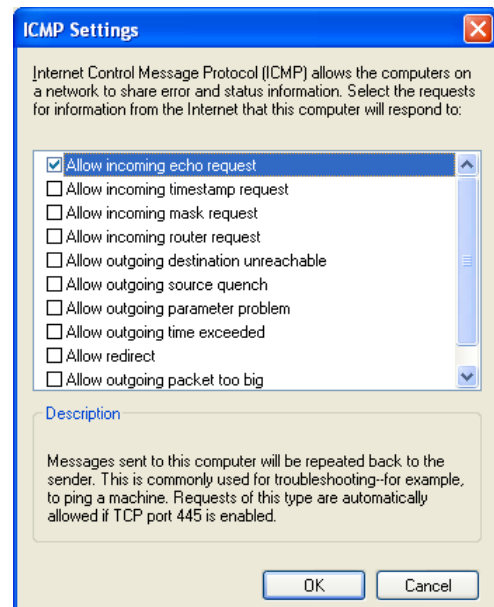
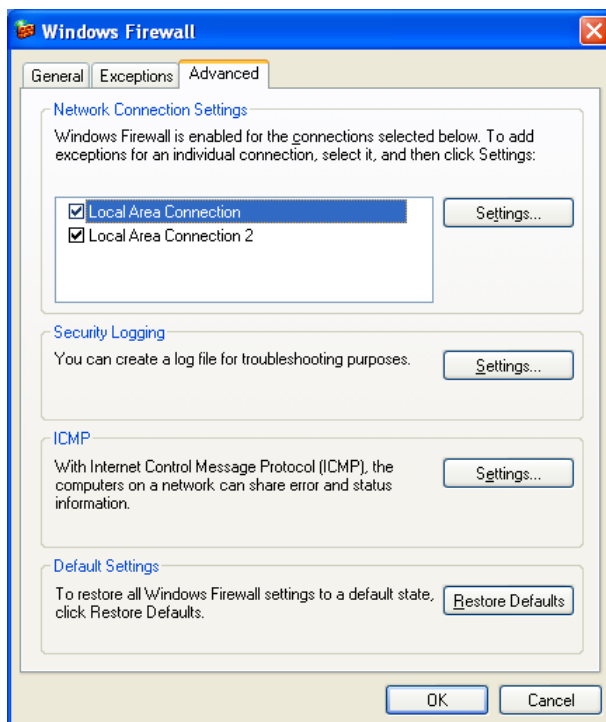
How to allow incoming echo requests (HG cameras)

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”

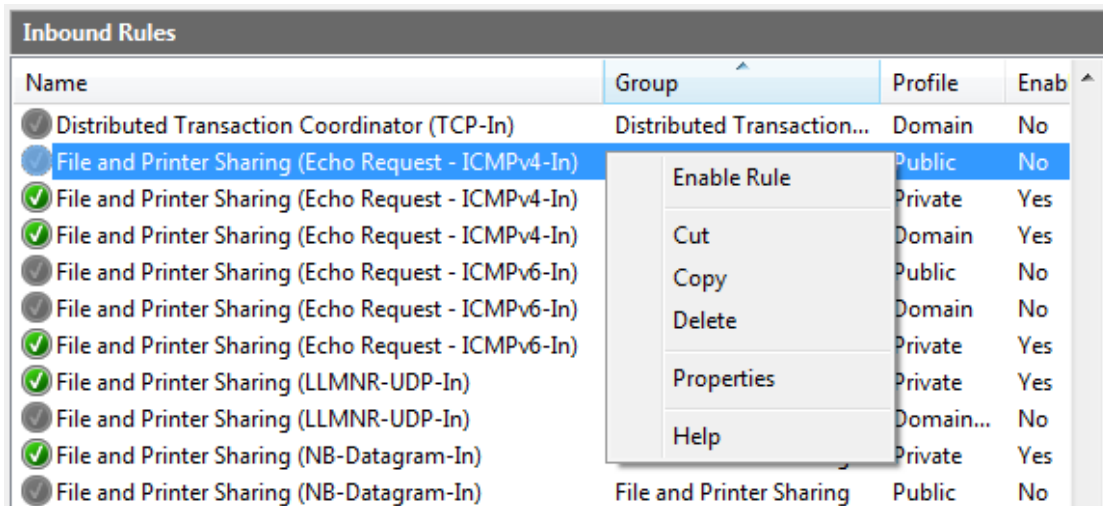
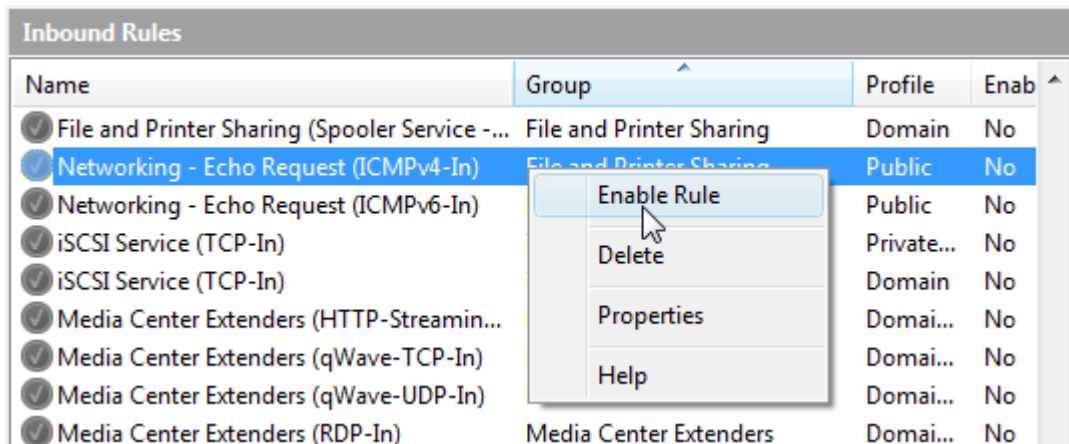


Click the ICMP settings and make sure that the “Allow incoming echo requests” option is selected.



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).



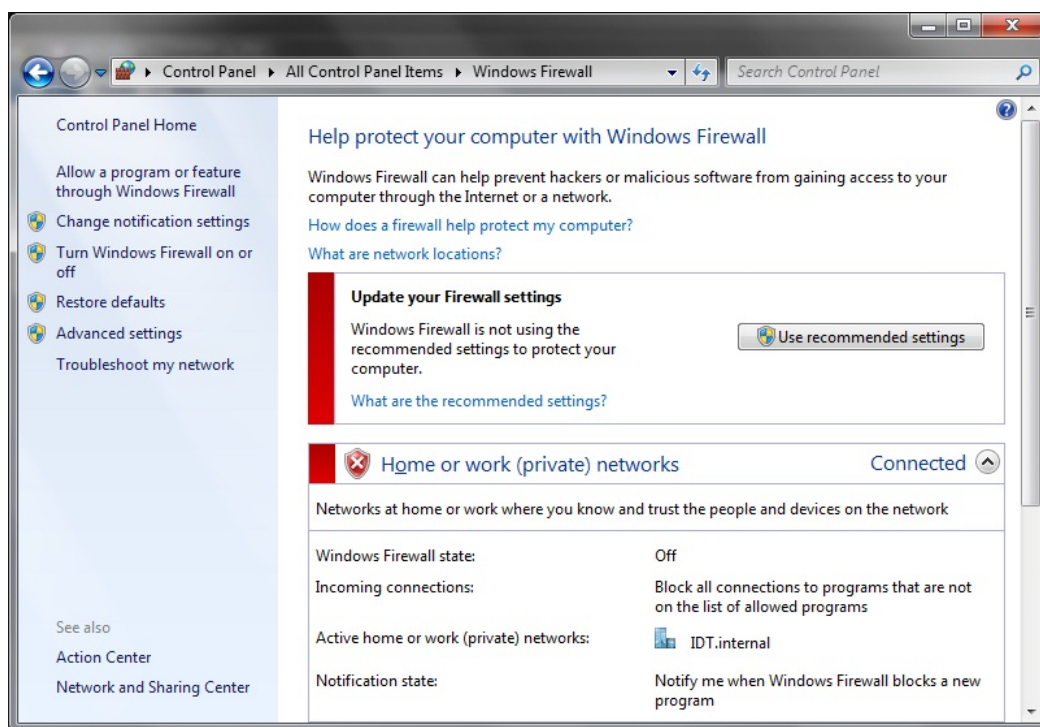
How to disable Windows firewall

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.

