

Setting Up Exclusions for iTEVA in Antivirus and Firewall Applications

Table of Contents

Adding Exception for Instrument Connection in Windows Firewall2

Adding Exception for Instrument Connection in Norton Security Suite4

Excluding the Instrument Connection in Other Firewall Applications7

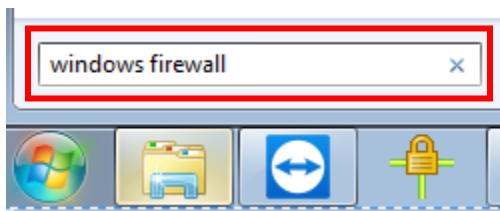
Adding Exception for iTEVA software folders in Norton Security Suite8

Adding Exceptions for iTEVA in Other Antivirus or Antimalware Applications9

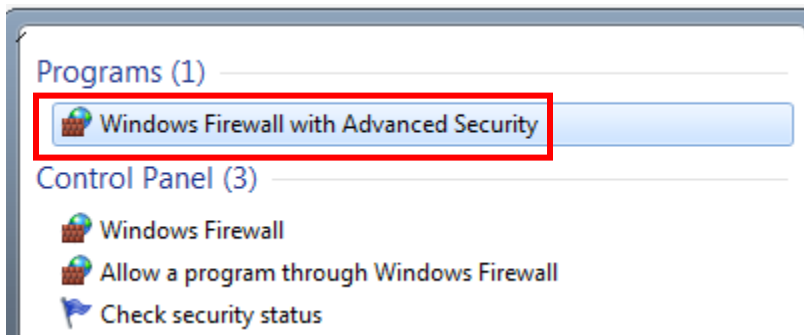
Adding Exception for Instrument Connection in Windows Firewall


Instead of having to go through the extra keystrokes necessary to create a rule in order to make an exception for the Instrument Connection, Windows Firewall allows one to exclude the Instrument Network Connection from altogether even being monitored in the first place. This can be done as follows:

- 1) Navigate to Windows Firewall. The quickest way to do this is by clicking on the Windows icon in the bottom left hand corner of the screen and then type “Windows Firewall” into the search box



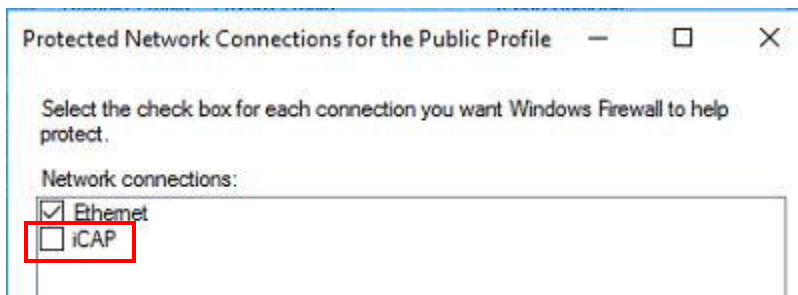
- 2) Click on **Windows Firewall with Advanced Security**



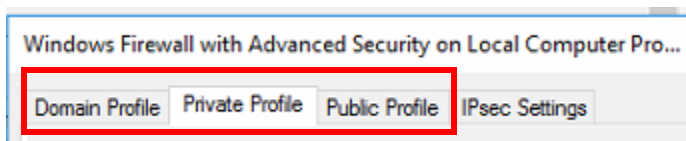
- 3) Click on  [Windows Firewall Properties](#)
- 4) Click on the **Customize** icon next to **Protected network connections**



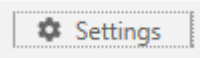
- 5) Uncheck the box next to the Instrument Network Connection



- 6) Repeat steps 4-5 for the Domain Profile and Private Profiles. In the end the Instrument Network Connection needs to be deselected for all three profiles: Domain, Private, Public.



Adding Exception for Instrument Connection in Norton Security Suite

- 1) Click 
- 2) Click **Firewall**
- 3) Click **Traffic Rules**
- 4) Click **Add**
- 5) Select the radio button for **Allow: Allow connections that match this rule**

Do you want to block, allow, or monitor a new connection?

 - Allow:** Allow connections that match this rule.
 - Block:** Do not allow connections that match this rule.
 - Monitor:** Log connections that match this rule. This lets you monitor the number of times this rule is used.
- 6) Click **Next >**
- 7) Select the radio button for **Connections to and from computers**

What type of connection do you want to **allow**?

 - Connections **to** other computers
Type of connection made by most Internet-enabled applications. Also called outbound connections.
 - Connections **from** other computers
Type of connection typical of a server application such as a Web server or FTP server. Also called inbound connections.
 - Connections **to and from** other computers
Some applications utilize both type of connections (inbound and outbound).
- 8) Select radio button for **Only the computers and sites listed below**

What computers or sites do you want to **allow** access to?

 - Any computer
 - Any computer in the local subnet
 - Only the computers and sites listed below:
- 9) Click **Add**

- 10) Select the radio button for **Using a network address** and then type **90.0.0.50** into **Network address** field and **255.255.255.0** into **Subnet mask** field.

Indicate computers or sites to **allow** access to:

- Individually
 Using a range
 Using a network address

Network address (example: 192.168.1.0)

90.0.0.50

Subnet mask (example: 255.255.255.0)

255.255.255.0

- 11) Click **Next >**

- 12) Select **TCP** from the drop down menu for **protocol to allow** and then select the radio button for **The rule will apply only if it matches all of the ports listed below:**

The protocol you want to **allow**:

TCP

What types of communication, or ports, do you want to **allow**?

- All types of communication (all ports, local and remote)
 The rule will apply only if it matches all of the ports listed below:

- 13) Click **Add**

- 14) Select radio button **Individually specified ports** for **Filter by** and **Local** for **Locality** and then type "2002 3002 5002" into **port entry** field

Filter by:

Known ports from list

Individually specified ports

Port range

Locality:

Local

Remote

Enter port number or numbers. To enter multiple port numbers, use a space between each entry.

- 15) Click **OK**
- 16) Click **Next >** and then click **Next >** again
- 17) Name the rule

What do you want to call this rule?

This description appears in the Rule Summary list to help you identify this rule:

- 18) Click **Next >**
- 19) Click **Finish**
- 20) Click **Close**
- 21) Click **Yes** to save changes

Save Changes?

You have changed your settings. Do you want to save these changes?



Yes **No**

Excluding the Instrument Connection in Other Firewall Applications

If you are setting up an exclusion for the instrument connection in an application which has not been demonstrated in this technical note, an exception can be made in that particular application using the following basic information which will apply to all Firewall and Host Intrusion applications.

Instrument Connection

Exclusion will need to be made for the following network (IP) address, subnet mask (if specified in application), and Local ports:

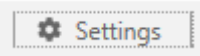

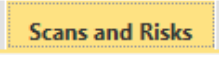




Network (IP) address: 90.0.0.50

Subnet Mask: 255.255.255.0

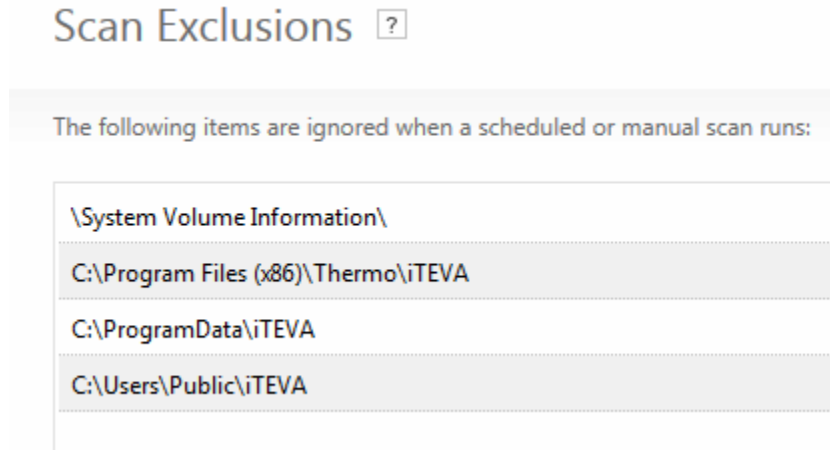
Local ports: 2002, 3002, 5002

Adding Exception for iTEVA software folders in Norton Security Suite

If there will be Antivirus or Antimalware programs which periodically scan the computer for presence of threats, it will be necessary to set exceptions for the folders which iTEVA uses so that they aren't scanned. Otherwise, if iTEVA is reading and/or writing to one of these folders while it is also being scanned by an Antivirus or Antimalware program, an application error could occur in iTEVA which could for instance cause a sequence to be interrupted. In this example, setting up exclusions will be demonstrated in Norton Security.

- 1) Click 
 - 2) Click 
 - 3) Click 
 - 4) In the row for **Items to Exclude from Scans**, Click 
 - 5) Click 
 - 6) In the **Add Item** popup window, Click , navigate to: **C:\Program Files\Thermo\iTEVA**, and click .
- Note:** In Windows 7 64bit, the iTEVA folder will be found in **Program Files (x86)**
- Note 2:** Please make sure that the **Include subfolders** checkbox is checked before clicking OK
- Include subfolders**
- 7) Repeat step 3-6 for the file path: **C:\ProgramData\iTEVA**
 - 8) Repeat step 3-6 for the file path: **C:\Users\Public\iTEVA**

9) The Exclusion list will look similar to that in the following screen capture:



Adding Exceptions for iTEVA in Other Antivirus or Antimalware Applications

If you are adding exceptions for iTEVA in another Antivirus or Antimalware program not demonstrated in this technical note, the same principle demonstrated for Norton Security Suite will apply. Add exceptions for the following folders in the program you are using:

C:\Program Files\Thermo\iTEVA
C:\ProgramData\iTEVA
C:\Users\Public\iTEVA