



On a PC with the OfficeShield Client installed right click on the Norton Internet Security 2010 system tray icon and select Norton Internet Security, then click Settings in the Network box:

**Norton Internet Security** Leave Feedback Norton Account Help & Support ▶

**Computer** [Settings](#)

[Scan Now ▶](#)  
[History & Quarantine](#)

[Run LiveUpdate](#) **3 minutes ago ▶**

**Insight Protection** [Details](#)  On *i*

**Antivirus**  On *i*

**Antispyware**  On *i*

**SONAR Protection**  On *i*

**Network** [Settings](#)

[Vulnerability Protection](#)  
[Network Security Map](#)

**Smart Firewall**  On *i*

**Intrusion Prevention**  On *i*

**Email Protection**  On *i*

**Web** [Settings](#)

[Log-ins & Cards](#)  
[Parental Controls](#)

**Identity Safe**  On *i*

**Browser Protection**  On *i*

**Safe Surfing**  On *i*

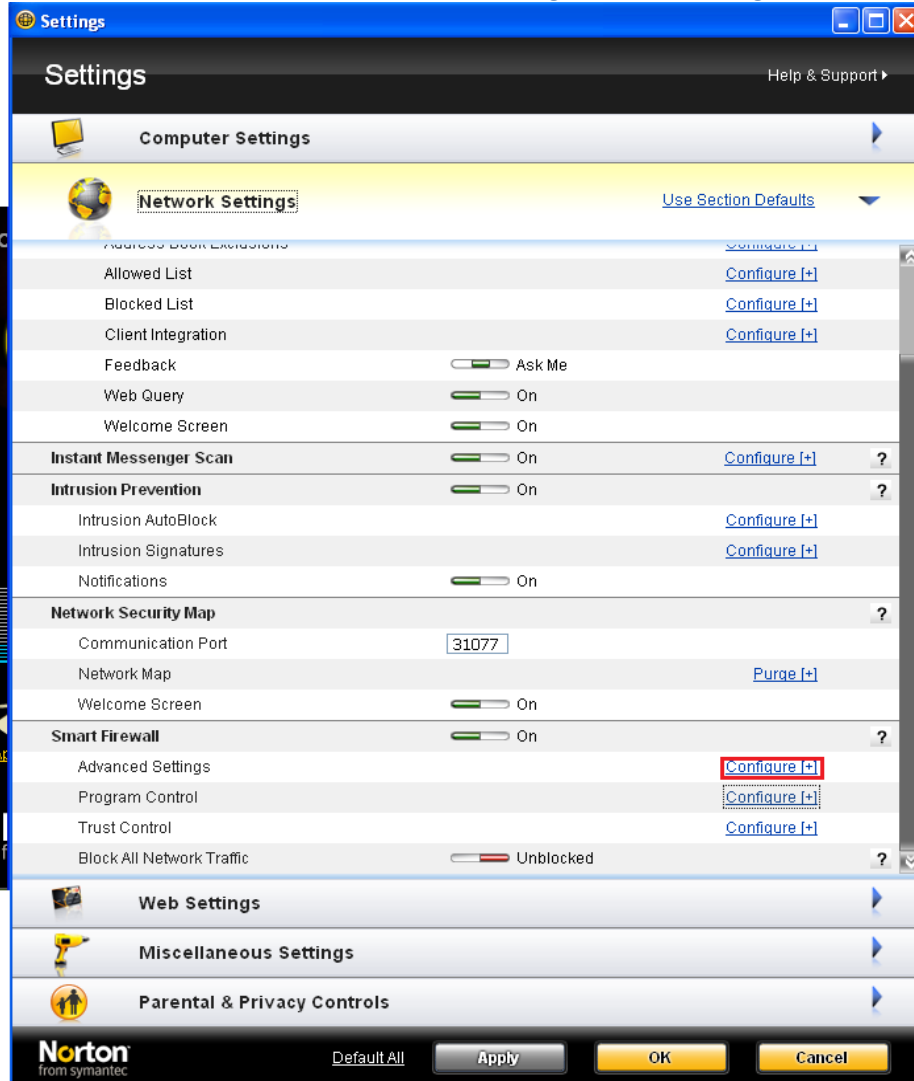
**Download Intelligence**  On *i*

**Norton**  
from symantec

You have **30 days of subscription remaining** [Subscribe Now](#)



Scroll down to the Smart Firewall, Advanced Settings and click Configure[+]:





Then click on General Rules -> Configure[+]:

Smart Firewall		
General Rules	<a href="#">Configure [+]</a>	?
Uncommon Protocols	<a href="#">Configure [+]</a>	?
Firewall Reset	<a href="#">Reset [+]</a>	?
Stealth Blocked Ports	<input checked="" type="checkbox"/> On	?
Stateful Protocol Filter	<input checked="" type="checkbox"/> On	?
Automatic File/Printer Sharing Control	<input checked="" type="checkbox"/> On	?
Automatic Program Control	<input checked="" type="checkbox"/> On	?
Automatic Learn IPv6 NAT Traversal Traffic	<input checked="" type="checkbox"/> On	?
Advanced Events Monitoring	<input type="checkbox"/> Off	?
Program Component	<a href="#">Configure [+]</a>	
Program Launch	<a href="#">Configure [+]</a>	
Command Line Execution	<a href="#">Configure [+]</a>	
Code Injection	<a href="#">Configure [+]</a>	
Window Messages	<a href="#">Configure [+]</a>	
Direct Network Access	<a href="#">Configure [+]</a>	
Active Desktop Change	<a href="#">Configure [+]</a>	
Key Logger Monitor	<a href="#">Configure [+]</a>	

**Norton** from symantec

[Default All](#)



Click Add (new rule):

General Rules

These rules determine how the firewall handles connections for all the programs on your computer. A rule that appears above other rules in the list overrides those rules.

		Description
<input type="checkbox"/>		Default Allow Specific Inbound ICMP <b>Allow</b> , Direction: Inbound, Computer: Any, Communications: Specific, Protocol: ICMP
<input checked="" type="checkbox"/>		Default Allow Specific Outbound ICMP <b>Allow</b> , Direction: Outbound, Computer: Any, Communications: Specific, Protocol: ICMP
<input checked="" type="checkbox"/>		Default Allow Inbound NetBIOS (Shared Networks) <b>Allow</b> , Direction: Inbound, Computer: Local subnet, Communications: Specific, Protocol: UDP <small>This rule is read-only</small>
<input checked="" type="checkbox"/>		Default Block Inbound NetBIOS <b>Block</b> , Direction: Inbound, Computer: Any, Communications: Specific, Protocol: UDP
<input checked="" type="checkbox"/>		Default Allow Inbound NetBIOS Name (Shared Networks) <b>Allow</b> , Direction: Inbound, Computer: Local subnet, Communications: Specific, Protocol: UDP
<input checked="" type="checkbox"/>		Default Block Inbound NetBIOS Name

**Add** View Remove Move Up Move Down

Norton from symantec OK Cancel



Choose Allow and click Next:

**Add Rule** Help

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.

**Norton**  
from symantec

< Back   **Next >**   Finish   Cancel



On next screen select “Connections from other computers” and click Next:

**Add Rule** Help

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).

**Norton**  
from symantec

< Back   **Next >**   Finish   Cancel



Choose "Any computer in the local subnet" and click Next

**Add Rule** [Close]

## Add Rule [Help](#)

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:

Type	Value
------	-------

**Norton**  
from symantec



On next screen choose TCP, then select “Only communications that match all types and ports listed below:” and click Add:

**Add Rule** Help

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)

Only communications that match all types and ports listed below:

Ports
-------

**Add** **Remove**

**Norton**  
from symantec

**< Back** **Next >** **Finish** **Cancel**





Make sure that “Known ports from list” and “Local” are selected, then check port number **135** and click OK:

**Specify Ports** ? Help

**Filter by:**

- Known ports from list
- Individually specified ports
- Port range

**Locality:**

- Local
- Remote

✓	Port	Name	Description
<input type="checkbox"/>	117	uucp-path	uucp-path
<input type="checkbox"/>	119	nntp	aka usenet, Network News Transfer Protocol
<input checked="" type="checkbox"/>	135	epmap	aka loc-srv, DCE endpoint resolution
<input type="checkbox"/>	137	netbios-ns	aka nbname, NETBIOS Name Service
<input type="checkbox"/>	139	netbios-ssn	aka nbssession, NETBIOS Session Service
<input type="checkbox"/>	143	imap	aka imap4, Internet Message Access Protocol
<input type="checkbox"/>	158	pcmail-srv	PCMail Server

**Norton**  
from symantec

OK Cancel



Then click Next, on the Advanced tab click Next, on the Descriptions tab enter the name for this rule (for example “RPC”); then click Finish to add this rule; Select your newly added rule and click “Move Up” repeatedly until it is on top of the list:

**General Rules** [Close]

## General Rules

[Help](#)

These rules determine how the firewall handles connections for all the programs on your computer. A rule that appears above other rules in the list overrides those rules.

<input checked="" type="checkbox"/>		Description
<input checked="" type="checkbox"/>		<b>RPC</b> <b>Allow</b> , Direction: Inbound, Computer: Local subnet, Communications: Specific, Protocol: TCP
<input type="checkbox"/>		Default Allow Specific Inbound ICMP <b>Allow</b> , Direction: Inbound, Computer: Any, Communications: Specific, Protocol: ICMP
<input checked="" type="checkbox"/>		Default Allow Specific Outbound ICMP <b>Allow</b> , Direction: Outbound, Computer: Any, Communications: Specific, Protocol: ICMP
<input checked="" type="checkbox"/>		Default Allow Inbound NetBIOS (Shared Networks) <b>Allow</b> , Direction: Inbound, Computer: Local subnet, Communications: Specific, Protocol: UDP
<input checked="" type="checkbox"/>		Default Block Inbound NetBIOS <b>Block</b> , Direction: Inbound, Computer: Any, Communications: Specific, Protocol: UDP
<input type="checkbox"/>		Default Allow Inbound NetBIOS Name (Shared Networks)

**Add** **Modify** **Remove** **Move Up** **Move Down**

**Norton**  
from symantec

**OK** **Cancel**