



Start the Norton Internet Security 2011 application and navigate to the Network Settings page. You will need to select Configure under the Smart Firewall - Advanced Settings

The screenshot shows the 'Settings' window for Norton Internet Security 2011. The 'Network Settings' section is highlighted in yellow. The 'Smart Firewall' section is expanded, and the 'Advanced Settings' option is highlighted with a red box around its 'Configure [+]' button. The 'Block All Network Traffic' option is set to 'Unblocked'.

Setting	Status	Action
Welcome Screen	On	
Instant Messenger Scan	On	<a href="#">Configure [+]</a>
Intrusion Prevention	On	<a href="#">?</a>
Intrusion AutoBlock		<a href="#">Configure [+]</a>
Intrusion Signatures		<a href="#">Configure [+]</a>
Notifications	On	
Exclusion List		<a href="#">Purge [+]</a>
Network Security Map		<a href="#">Purge [+]</a> <a href="#">?</a>
Communication Port	31077	
Welcome Screen	On	
Smart Firewall	On	<a href="#">?</a>
Advanced Settings		<a href="#">Configure [+]</a>
Program Control		<a href="#">Configure [+]</a>
Trust Control		<a href="#">Configure [+]</a>
Block All Network Traffic	Unblocked	<a href="#">?</a>



On the advanced settings page select Configure under General Rules.

**Advanced Settings** Help

**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>	
COM Control	<a href="#">Configure [+]</a>	

**Norton** by Symantec Default All Apply OK Cancel



On the General Rules page you will need to add a new Firewall Rule

The screenshot shows the 'General Rules' window in Norton Firewall. The window title is 'General Rules' and it has a 'Help' link in the top right. Below the title bar, there is a header 'General Rules' and a 'Help' link. The main content area contains a list of rules with checkboxes and icons. The first rule, 'Default Allow Specific Inbound ICMP', is highlighted in yellow. Below the list are buttons for 'Add', 'View', 'Remove', 'Move Up', and 'Move Down'. The 'Add' button is highlighted with a red box. At the bottom of the window, there is a Norton by Symantec logo and 'OK' and 'Cancel' buttons.

✓	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 Inbound ICMP Destination Unreachable <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)



Set the rule to allow connections that match this rule.

**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.

< Back **Next >** Finish Cancel



Allow connections from other computers.

**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).

< Back **Next >** Finish Cancel



Select any computer in the local subnet.

**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
------	-------



Set the protocol to Allow TCP and check the radio button to only allow communications that match all types and ports listed

**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

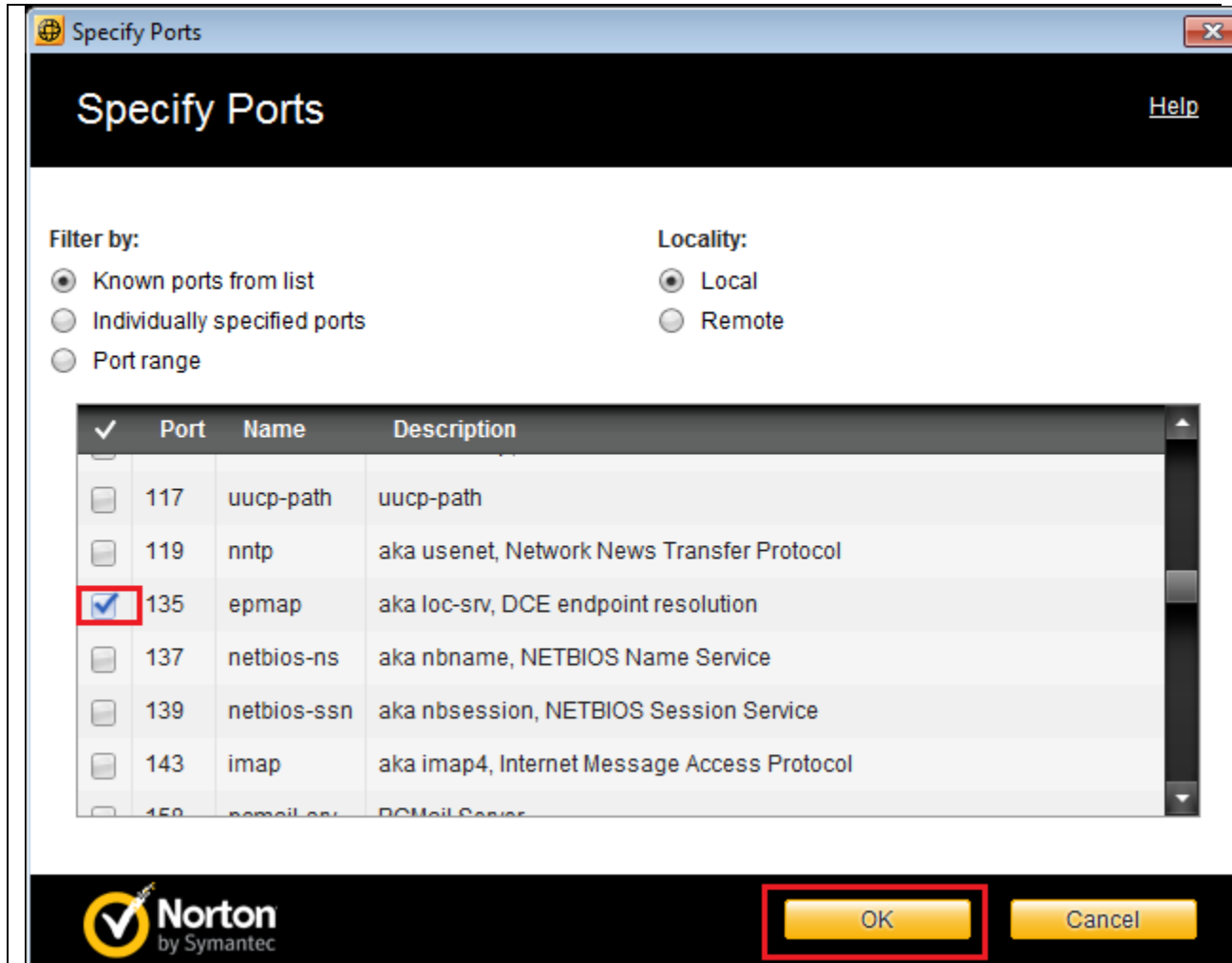
Add Remove

**Norton**  
by Symantec

< Back Next > Finish Cancel



Select port 135 from the list of Known ports and select OK





Once back at the Add Rule screen your new port should be listed below, select Next

**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
local epmap (port 135)



Select next

**Add Rule** [Help](#)

When a connection matches a rule:

Create a Security History log entry

When packet is from NAT traversal (e.g. Teredo):

Apply this rule



Describe the rule so you are able to identify it at a later time. We recommend using OfficeShield or OS

**Add Rule** Help

What do you want to call this rule?  
This description appears in the Rule Summary list to help you identify this rule:



Click finish to add the new rule

**Add Rule**

You have created the following rule for Internet communications:

Description: OS  
Action: **Allow**  
Direction: Inbound  
Computer: Local subnet  
Communications: Specific  
Protocol: TCP

**Creating a new general rule will override all application rules, and should only be performed by advanced users or at the direction of tech support.**



Move the new OfficeShield rule to the top

The screenshot shows the 'General Rules' window in Norton OfficeShield. The window title is 'General Rules' and it includes a 'Help' link. Below the title bar, there is an explanatory text: '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"/>	Default Allow Web Services Discovery (Shared Networks) <b>Allow</b> , Direction: Inbound, Computer: Local subnet, Communications: Specific, Protocol: UDP
<input checked="" type="checkbox"/>	Default Block Web Services Discovery <b>Block</b> , Direction: Inbound, Computer: Any, Communications: Specific, Protocol: UDP, Tracking: Create a log entry
<input checked="" type="checkbox"/>	Default Allow SSDP (Shared Networks) <b>Allow</b> , Direction: Inbound, Computer: Local subnet, Communications: Specific, Protocol: TCP
<input checked="" type="checkbox"/>	Default Block SSDP <b>Block</b> , Direction: Inbound, Computer: Any, Communications: Specific, Protocol: TCP, Tracking: Create a log entry
<input checked="" type="checkbox"/>	OS <b>Allow</b> , Direction: Inbound, Computer: Local subnet, Communications: Specific, Protocol: TCP

Below the table, there are five buttons: 'Add', 'Modify', 'Remove', 'Move Up', and 'Move Down'. The 'Move Up' button is highlighted with a red rectangular border. At the bottom of the window, there is the Norton by Symantec logo and two buttons: 'OK' and 'Cancel'.



Click OK, you have completed your configuration.

**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>OS</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 Inbound ICMP Destination Unreachable <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 type="checkbox"/>	Default Block Inbound NetBIOS