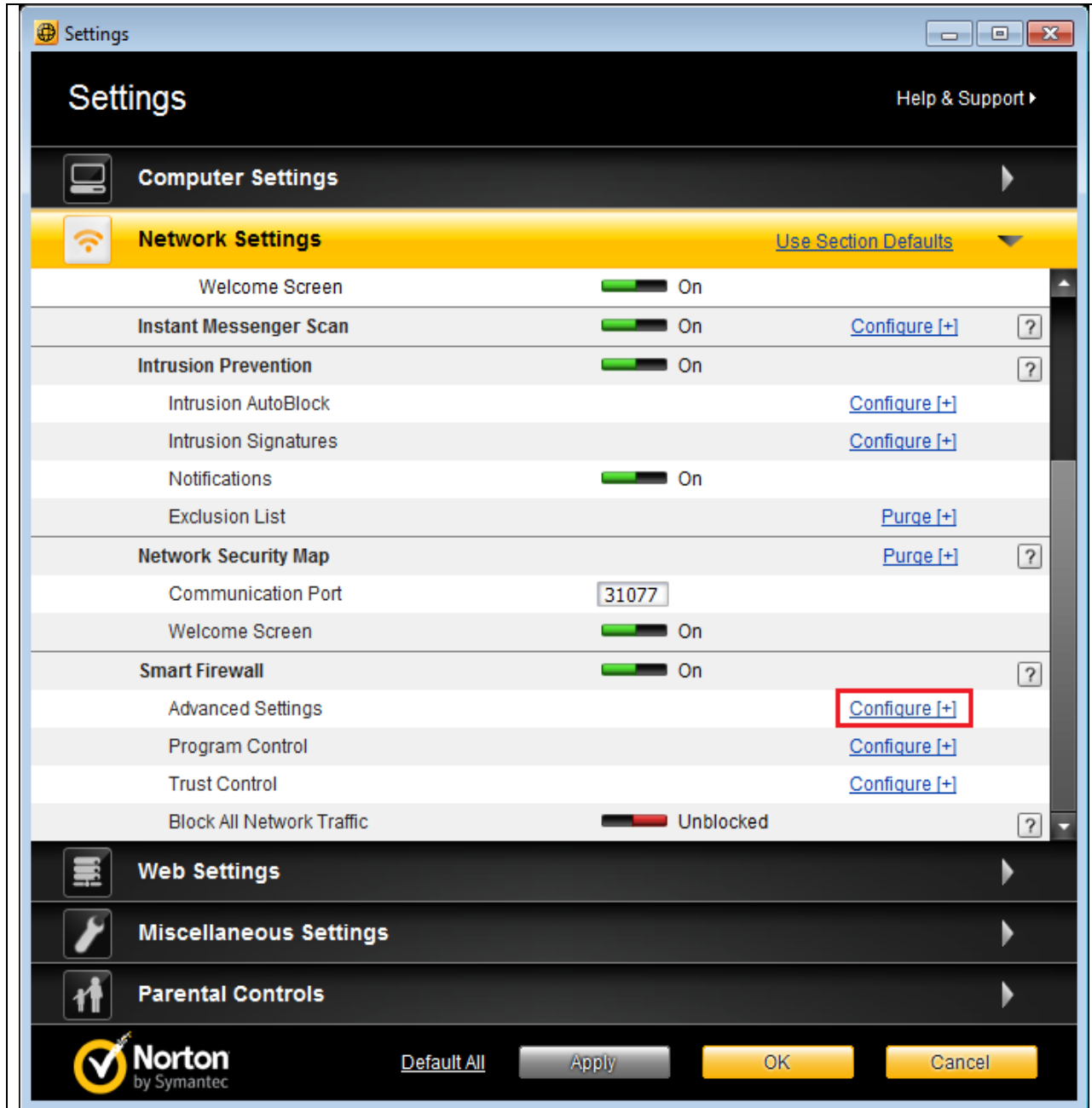




Start the Norton Internet Security 2011 application and navigate to the Network Settings page. You will need to select Configure under the Smart Firewall - Advanced Settings





On the advanced settings page select Configure under General Rules.

Advanced Settings Help

Smart Firewall

General Rules	Configure [+]	?
Uncommon Protocols	Configure [+]	?
Firewall Reset	Reset [+]	?
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	Configure [+]	
Program Launch	Configure [+]	
Command Line Execution	Configure [+]	
Code Injection	Configure [+]	
Window Messages	Configure [+]	
Direct Network Access	Configure [+]	
Active Desktop Change	Configure [+]	
Key Logger Monitor	Configure [+]	
COM Control	Configure [+]	

[Default All](#)



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

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

Add **View** **Remove** **Move Up** **Move Down**

Norton by Symantec **OK** **Cancel**



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.



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

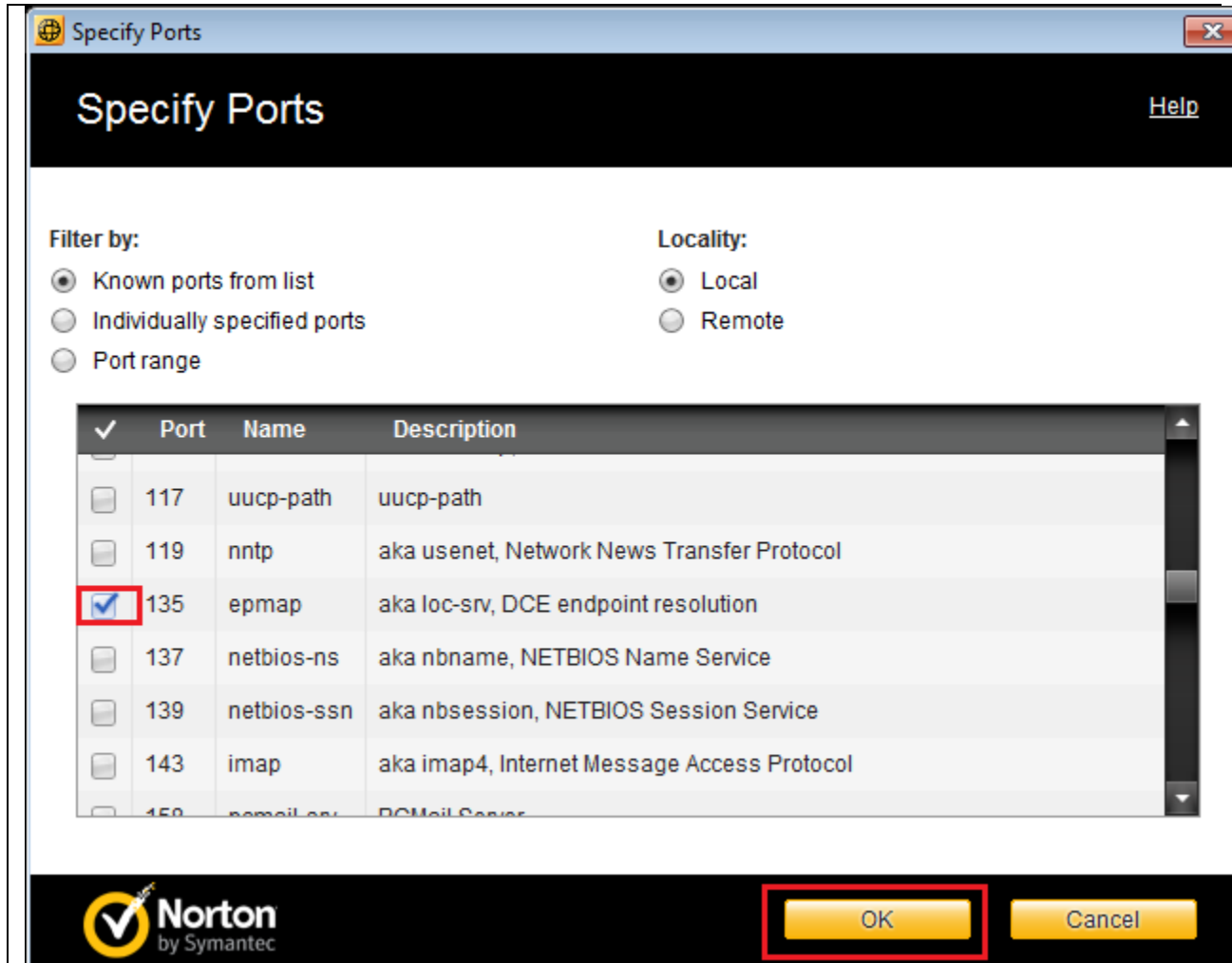
Add Remove

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



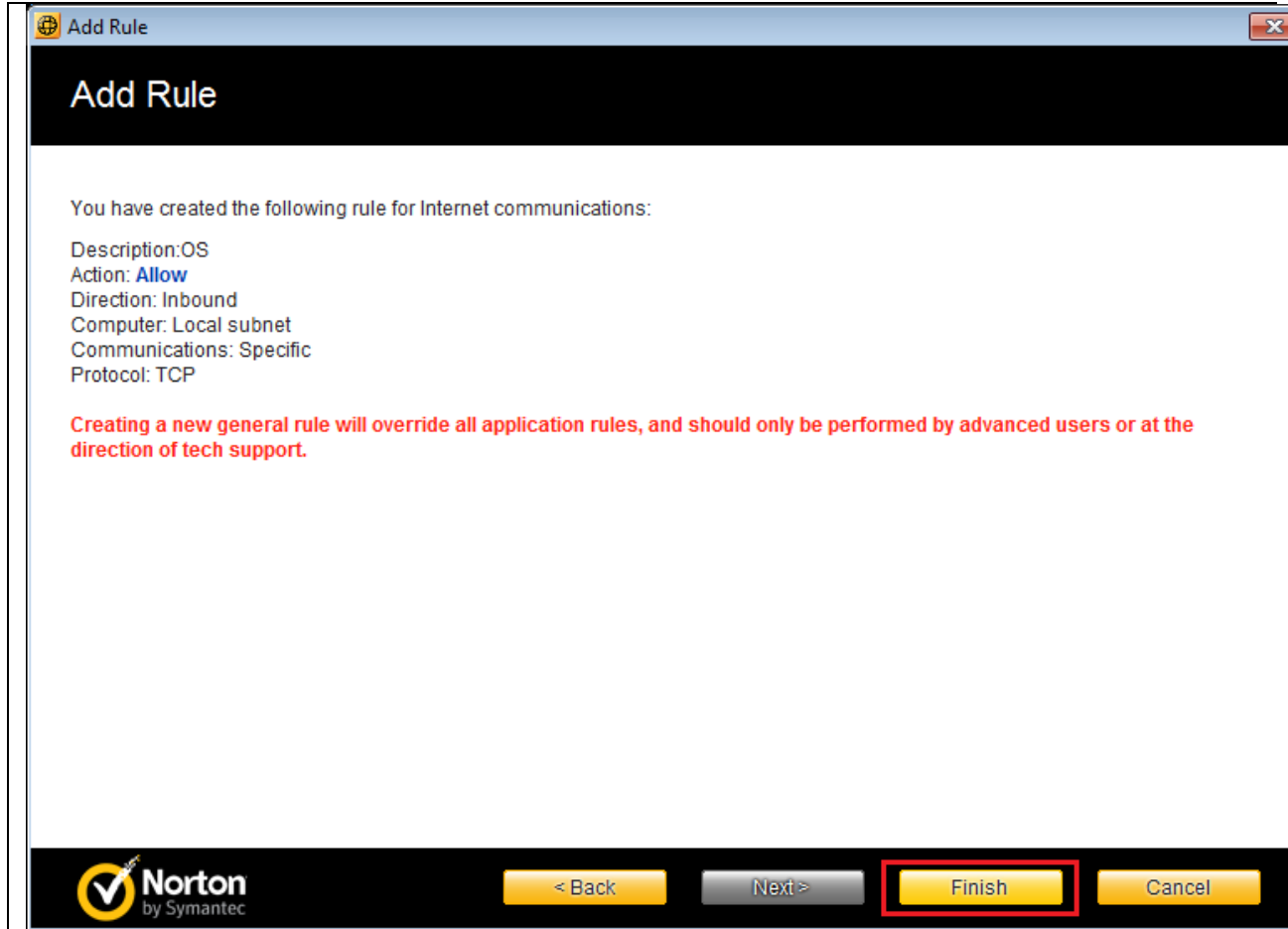
Describe the rule so you are able to identify it at a later time. We recommend using OfficeShield or OS

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





Move the new OfficeShield rule to the top

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"/>	Default Allow Web Services Discovery (Shared Networks) Allow , Direction: Inbound, Computer: Local subnet, Communications: Specific, Protocol: UDP
<input checked="" type="checkbox"/>	Default Block Web Services Discovery Block , Direction: Inbound, Computer: Any, Communications: Specific, Protocol: UDP, Tracking: Create a log entry
<input checked="" type="checkbox"/>	Default Allow SSDP (Shared Networks) Allow , Direction: Inbound, Computer: Local subnet, Communications: Specific, Protocol: TCP
<input checked="" type="checkbox"/>	Default Block SSDP Block , Direction: Inbound, Computer: Any, Communications: Specific, Protocol: TCP, Tracking: Create a log entry
<input checked="" type="checkbox"/>	OS Allow , Direction: Inbound, Computer: Local subnet, Communications: Specific, Protocol: TCP



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