

# Windows XP SP2 and the Windows Firewall

- Firewall on by default
- Operates on all interfaces
- Screens inbound traffic
- Does not screen outbound traffic
  - Minor exception is some ICMP message types

Net result is that by default almost all unsolicited attempts to connect to the workstation are blocked, but any program running on the system (including trojans) can connect outwards!

# Exceptions

- Allow to system to accept connections, either defining them by
  - Ports
  - or
  - Programs
- All exceptions have a SCOPE

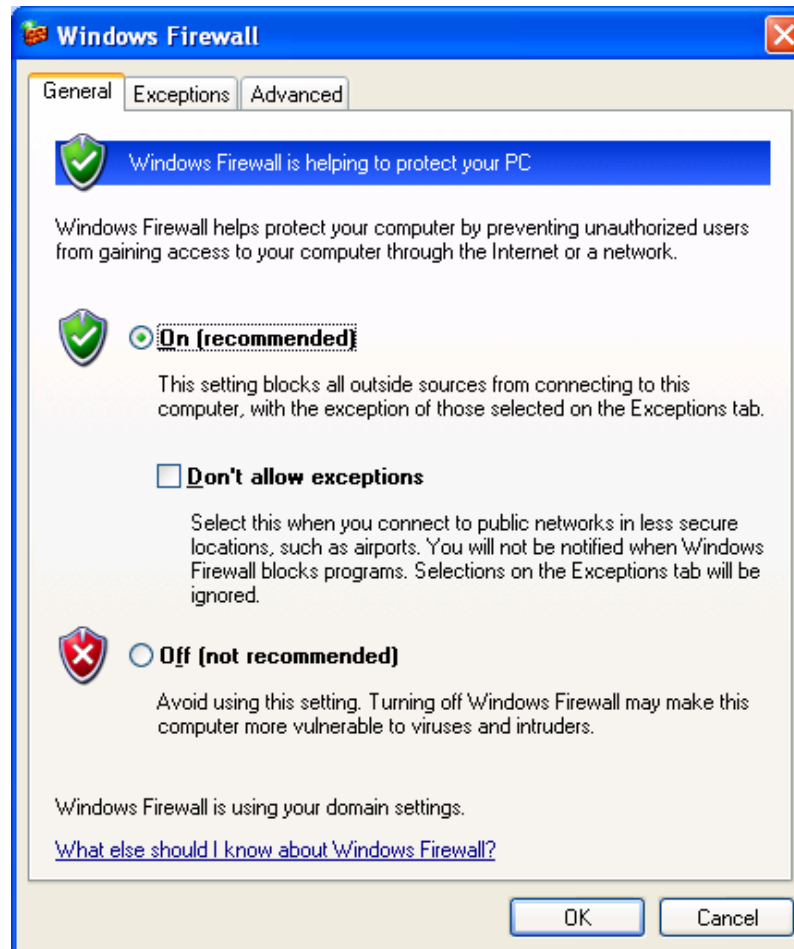
# Why Exceptions?

- File or print sharing
- Network management traffic
- Peer to peer collaboration
- Remote connection to workstations
  - Terminal services
  - VNC
  - Custom scripts

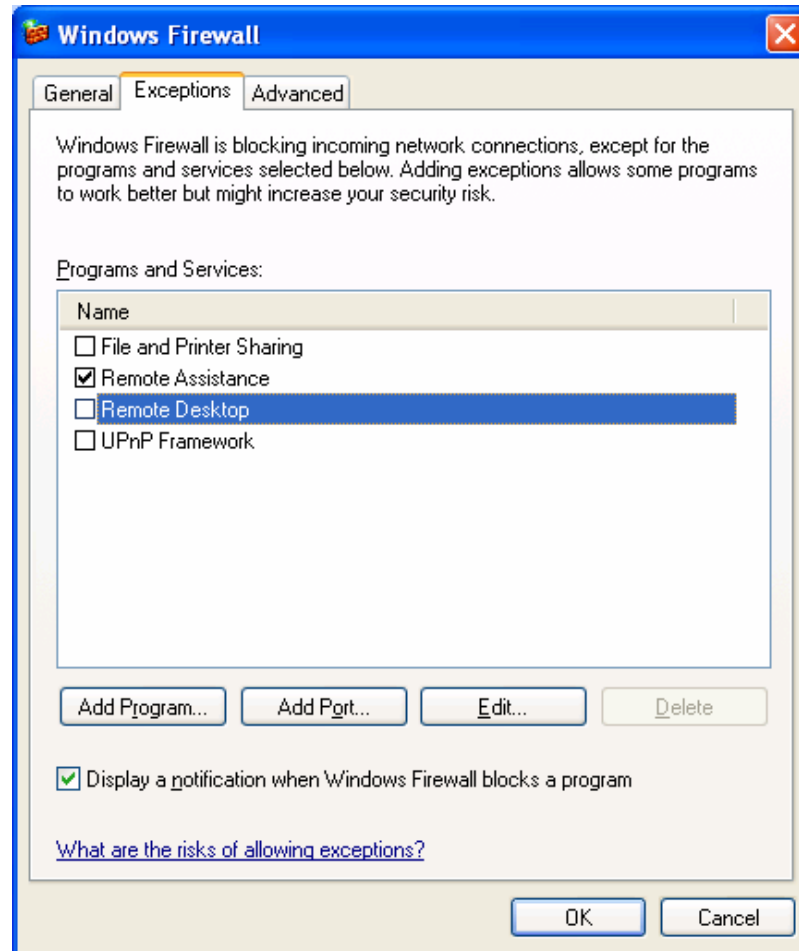
# Configuring the Firewall

- Firewall Control Panel
  - Local machine
  - Use to define machine specific settings
  - Allows setting for individual interfaces
- Group Policy
  - Preferable in large networks
- Scripts
  - Very versatile
  - New *netsh firewall* commands

# The Firewall Control panel

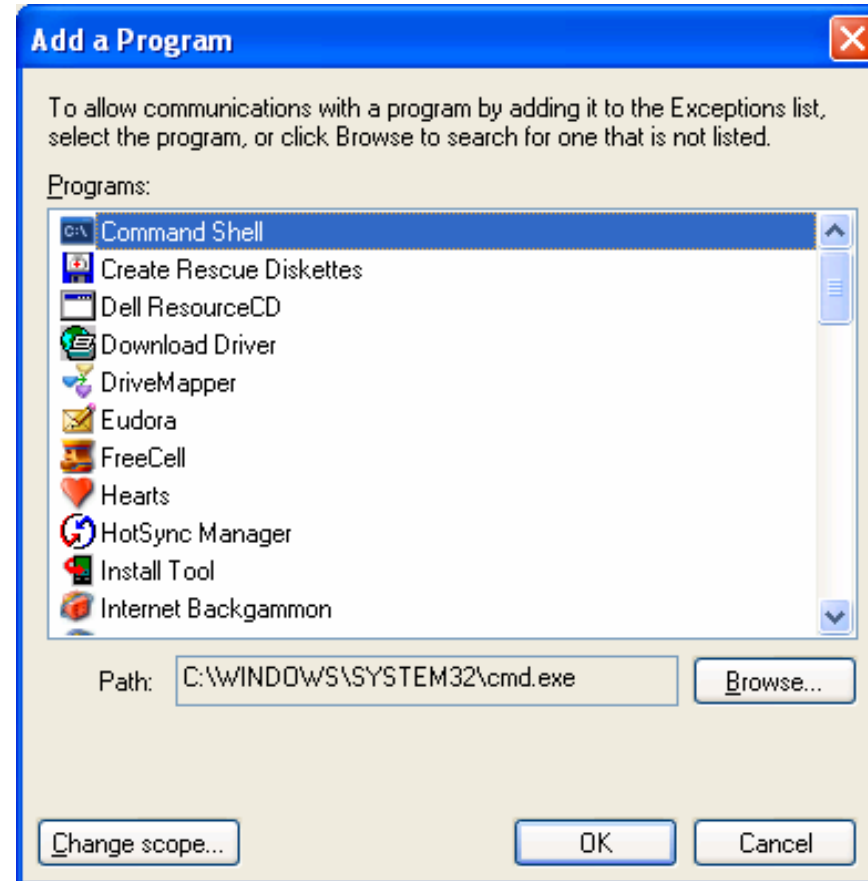


# The Exceptions Tab

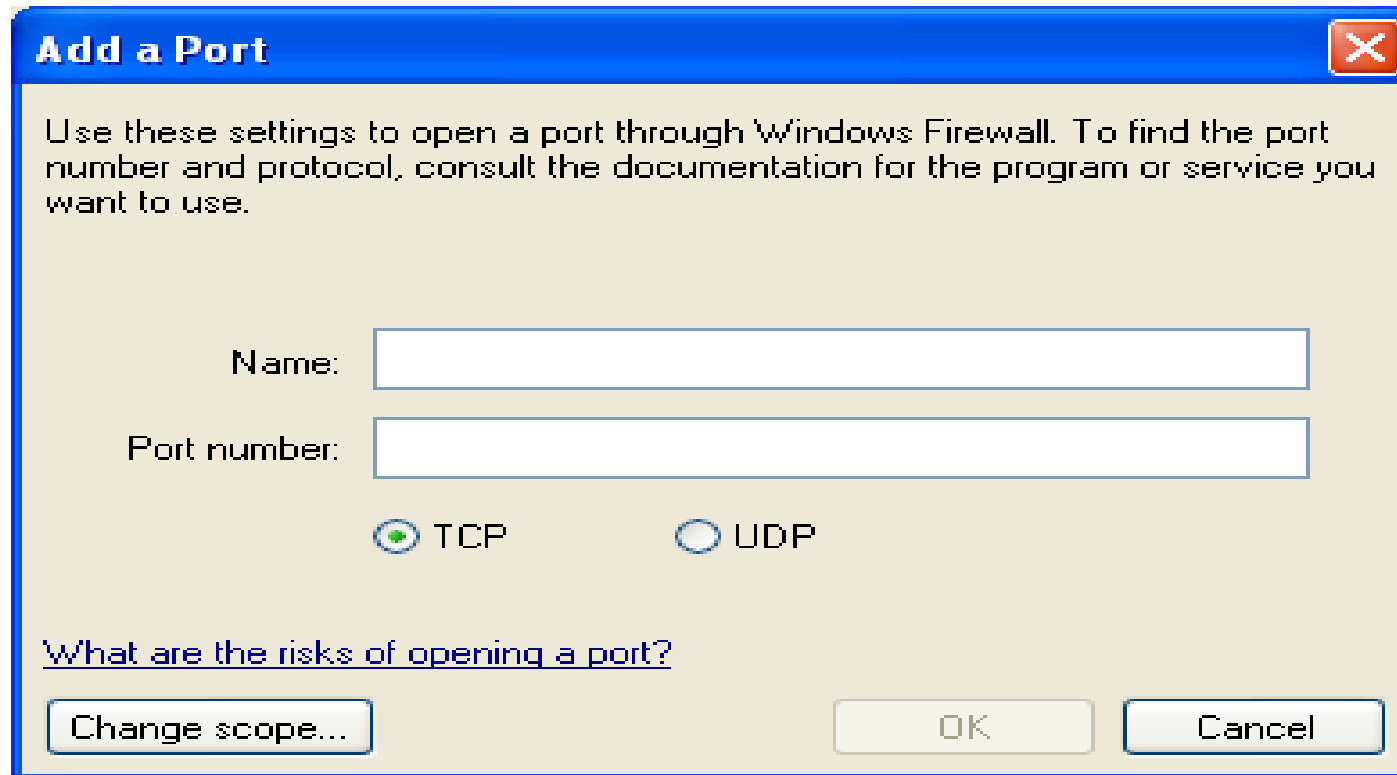


Pre-SP2 installed programmes may change this view.

# The *Add Programmes* Option



# The *Add Port* Option



**Add a Port** ✕

Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.

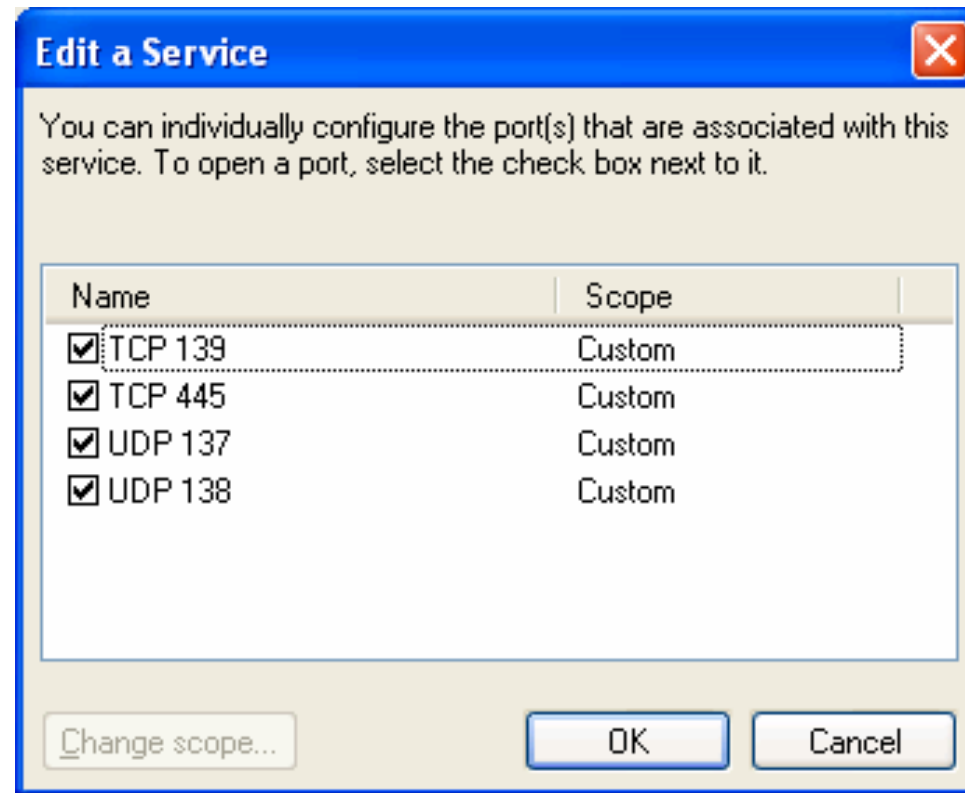
Name:

Port number:

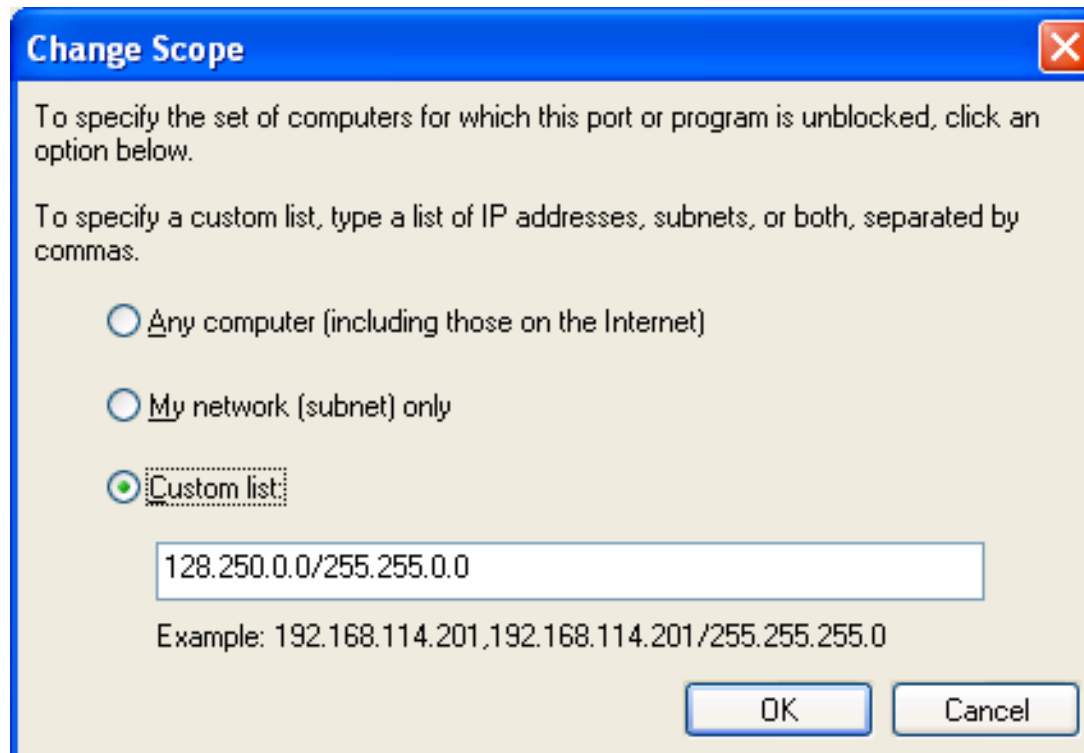
TCP       UDP

[What are the risks of opening a port?](#)

# Editing Existing Exceptions



# Scope



**Change Scope** [Close]

To specify the set of computers for which this port or program is unblocked, click an option below.

To specify a custom list, type a list of IP addresses, subnets, or both, separated by commas.

Any computer (including those on the Internet)

My network (subnet) only

Custom list:

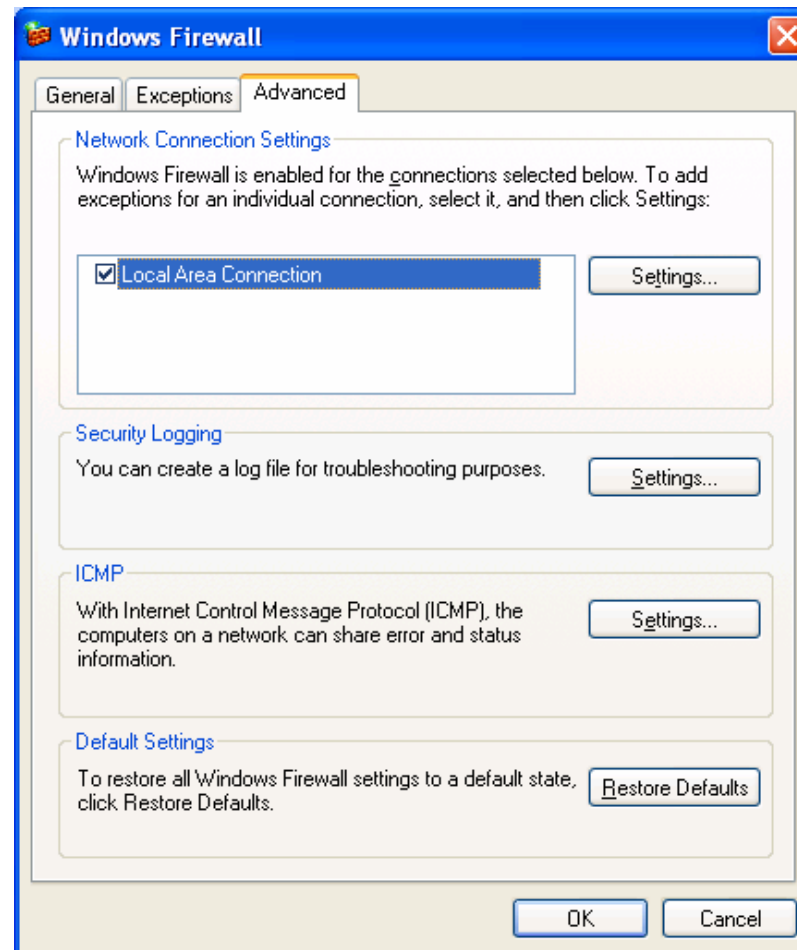
128.250.0.0/255.255.0.0

Example: 192.168.114.201,192.168.114.201/255.255.255.0

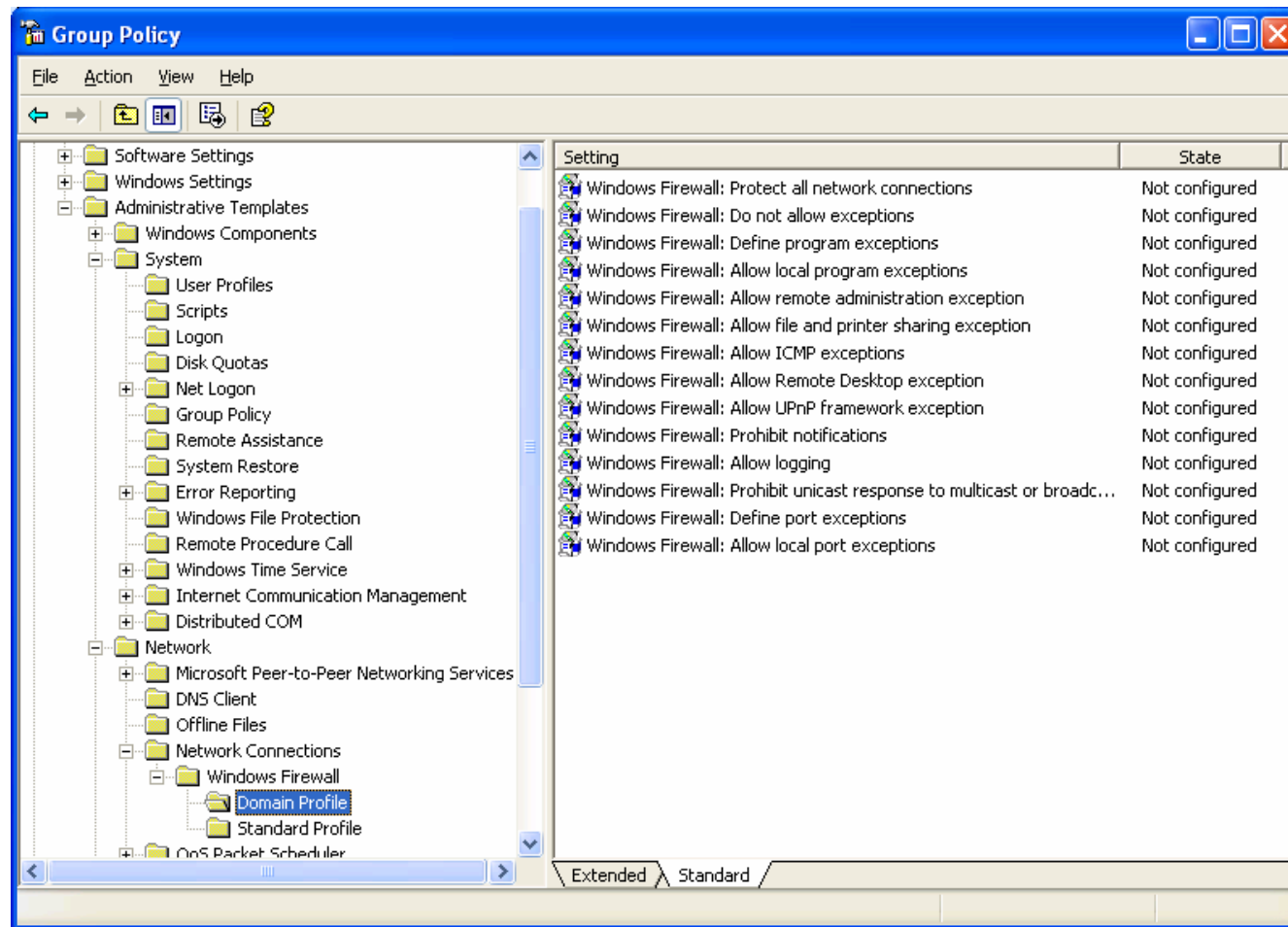
OK Cancel

The image shows a Windows-style dialog box titled "Change Scope". It has a blue title bar with a close button (red X) on the right. The main area is light beige. It contains two paragraphs of instructional text. Below the text are three radio button options: "Any computer (including those on the Internet)", "My network (subnet) only", and "Custom list:". The "Custom list:" option is selected, indicated by a green dot. Below this option is a text input field containing the IP address "128.250.0.0/255.255.0.0". Below the input field is an example of a custom list: "Example: 192.168.114.201,192.168.114.201/255.255.255.0". At the bottom right of the dialog are two buttons: "OK" and "Cancel".

# The Advanced Tab

















# Using Group Policy



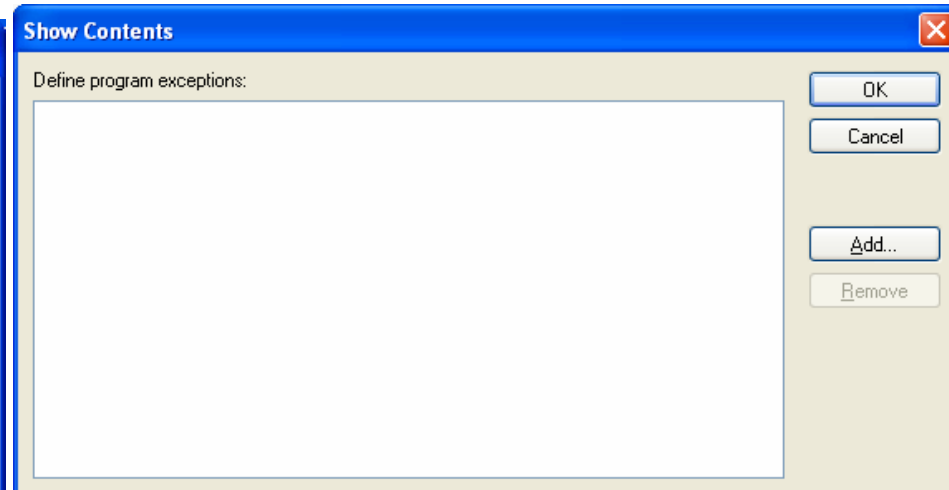
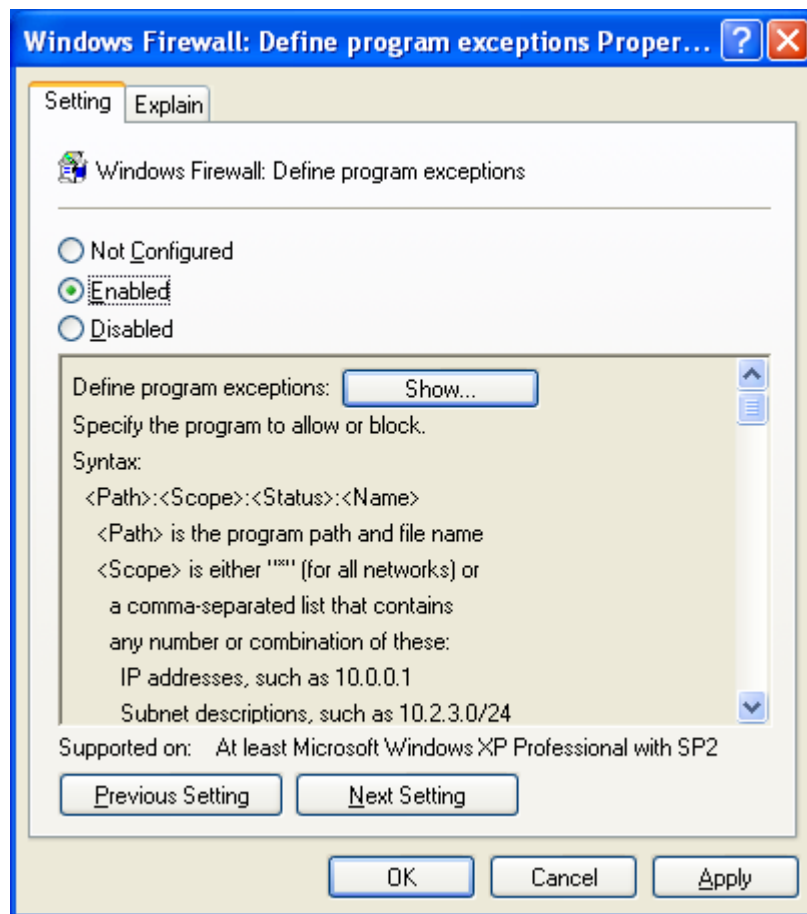
Note the 2 profiles – domain and standard

# The Parameters

---

 Windows Firewall: Protect all network connections	Not configured
 Windows Firewall: Do not allow exceptions	Not configured
 Windows Firewall: Define program exceptions	Not configured
 Windows Firewall: Allow local program exceptions	Not configured
 Windows Firewall: Allow remote administration exception	Not configured
 Windows Firewall: Allow file and printer sharing exception	Not configured
 Windows Firewall: Allow ICMP exceptions	Not configured
 Windows Firewall: Allow Remote Desktop exception	Not configured
 Windows Firewall: Allow UPnP framework exception	Not configured
 Windows Firewall: Prohibit notifications	Not configured
 Windows Firewall: Allow logging	Not configured
 Windows Firewall: Prohibit unicast response to multicast or broadcast	Not configured
 Windows Firewall: Define port exceptions	Not configured
 Windows Firewall: Allow local port exceptions	Not configured

# Define Programme Exceptions



A program exception is defined as such:

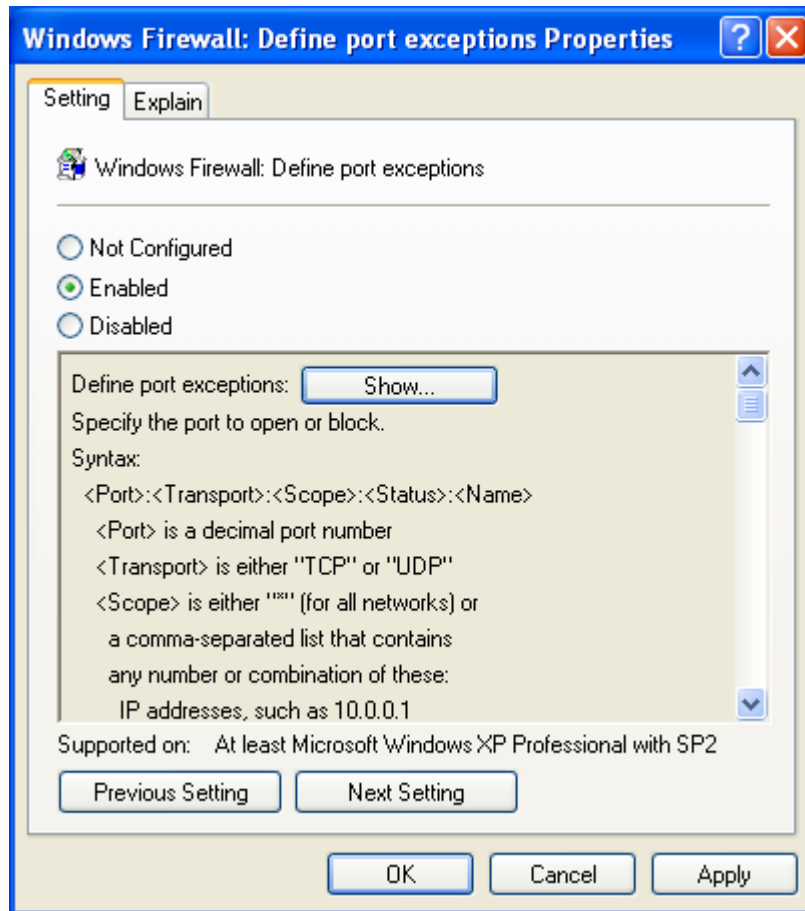
<path to the program>:<Scope>:<Status>:<Name>

**Scope** can be defined as \* for all source, or a list of ip addresses including LocalSubnet, single IP addresses (e.g. 128.250.6.90), or IP ranges (128.250.0.0/255.255.0.0 or 128.250.0.0/16).

An example would be:

C:\WINDOWS\system32\sessmgr.exe:LocalSubnet,128.250.6.64/26:enabled:remote control

# Define Port Exceptions



An example would be:

23:TCP:\*:enabled:telnet

Which would allow telnet connections from anywhere

# How do you know which exceptions are needed?

- By notification when a listening programme is installed
  - Not for services!
- Recognising required ports from dropped packet records in the logs

# Troubleshooting

- **netsh firewall show state verbose=enable**