IP Office Technical Tip

Bulletin no: 49

Release Date: 22 October 2004

Region: Global

Windows XP Service Pack 2 with IP Office Applications

Introduction

Microsoft Windows XP Service Pack 2 includes the Windows Firewall, a replacement for the Internet Connection Firewall (ICF) provided in previous versions of Windows XP. Windows Firewall is a stateful host-based firewall that discards unsolicited incoming traffic, providing a level of protection for computers against malicious users or programs. To provide better protection for computers connected to any kind of network, Windows XP SP2 enables Windows Firewall on all network connections by default.

This new behavior can impact the behaviour of many applications.

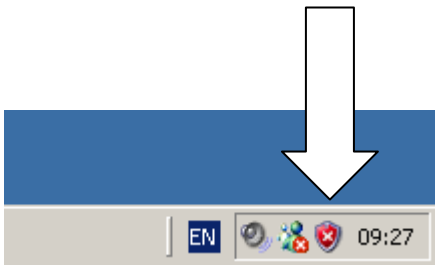
This document describes the changes appropriate to IP Office Applications to the configuration settings for Windows Firewall. Supplied with this document is a simple script file to install the appropriate Firewall Exceptions for the IP Office Applications. This is supplied on 'As-Is' basis, as some of the settings included in it may be overwritten by custom settings already on your computer or network.

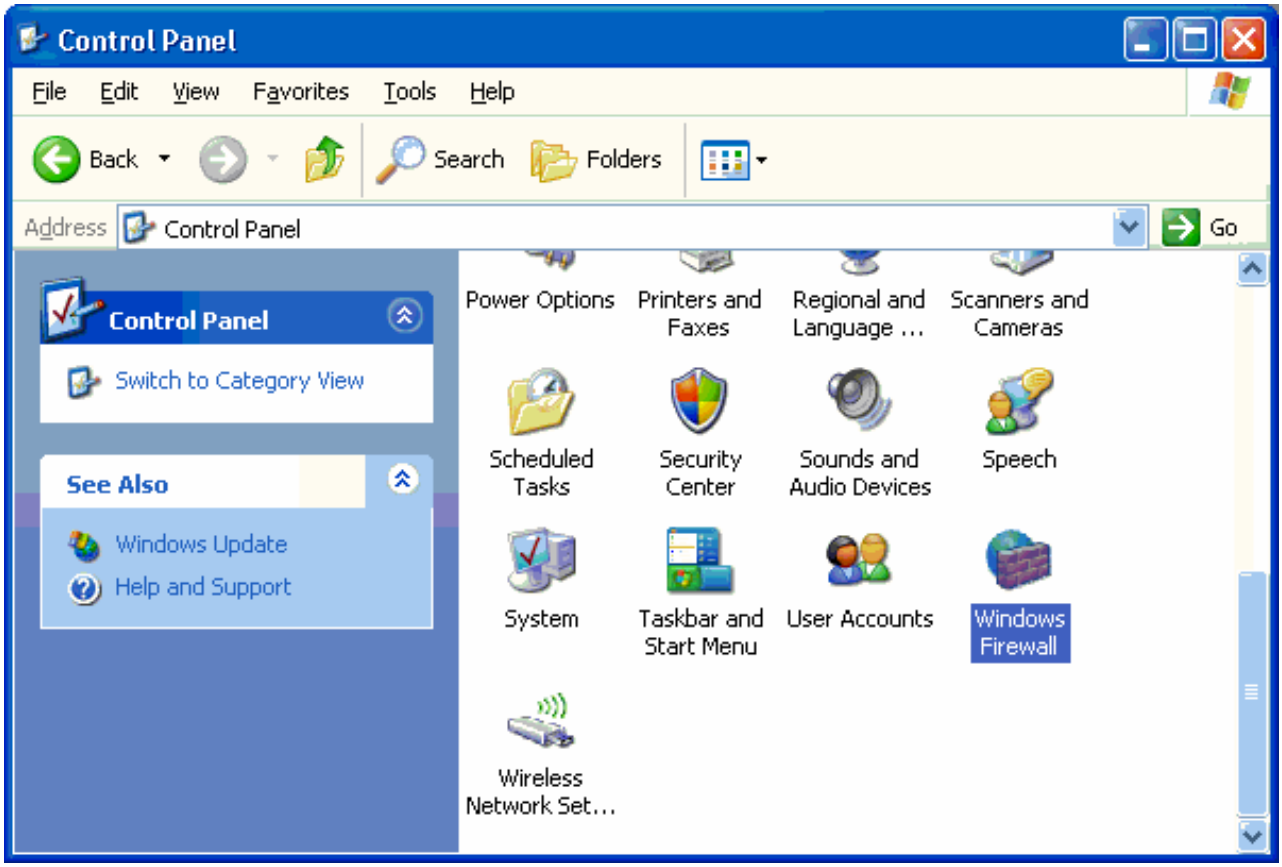
Security Alerts

Through continued use of applications, the Windows Firewall will generate the following Security Alert. At this point a user can select 'Unblock' to add the program into the firewall exception list. Please note that this is not always the complete solution to allow the application to operate correctly, as your computer may have custom settings already enabled, and further configuration may be required. You may need to speak to your systems administrator in order to modify these settings.

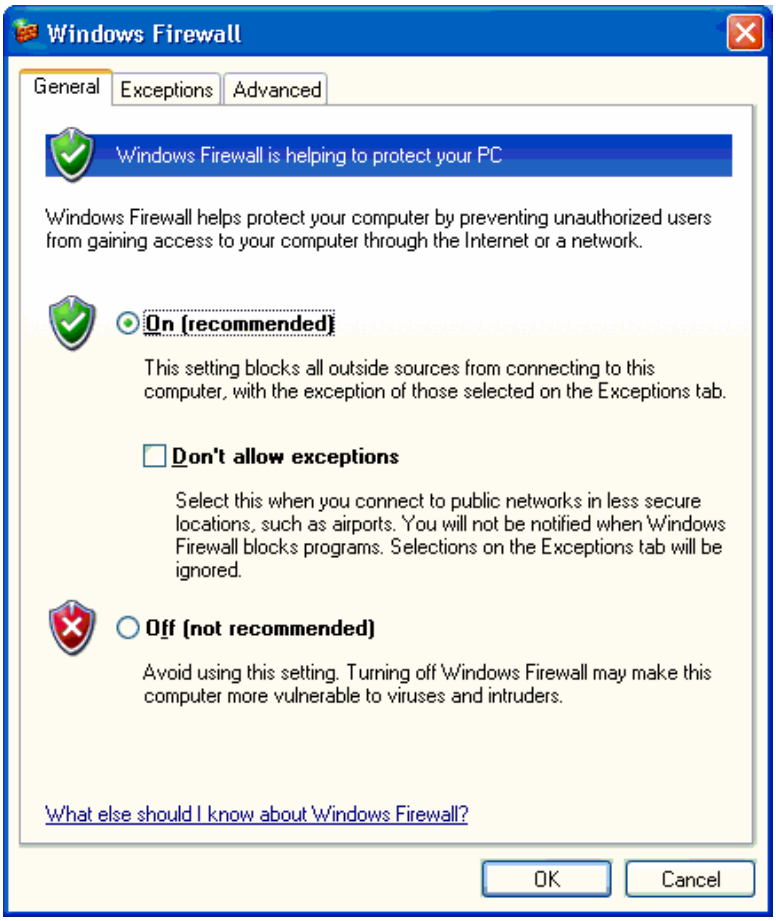
Firewall Configuration

From the control panel select the Windows Firewall icon. It is also possible to use the Security Centre Icon in the bottom right status toolbar

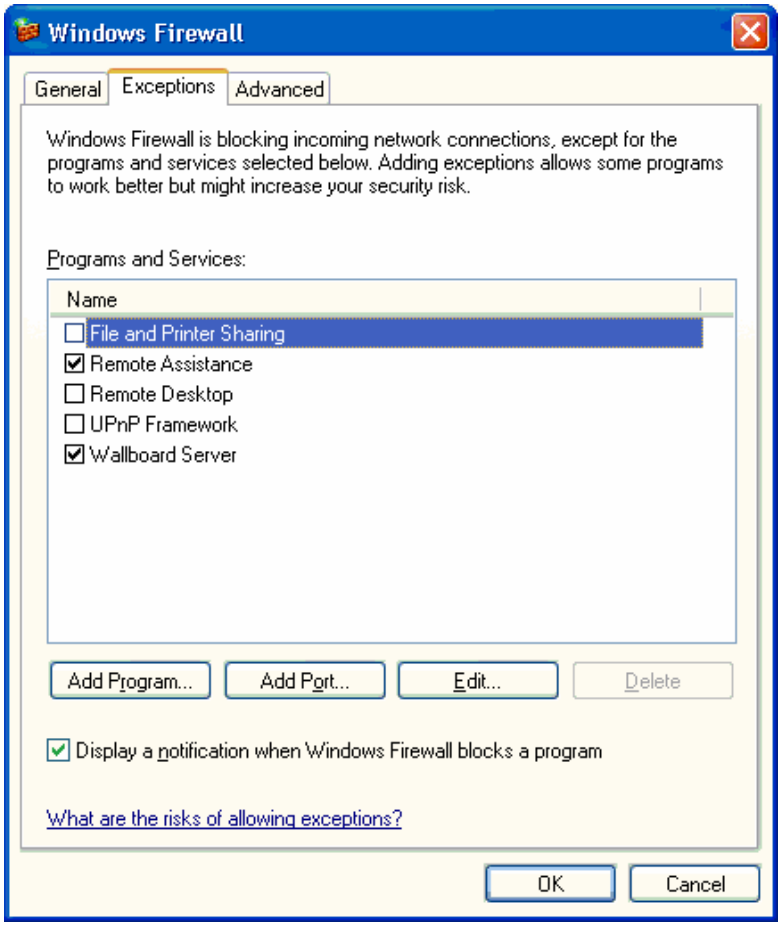




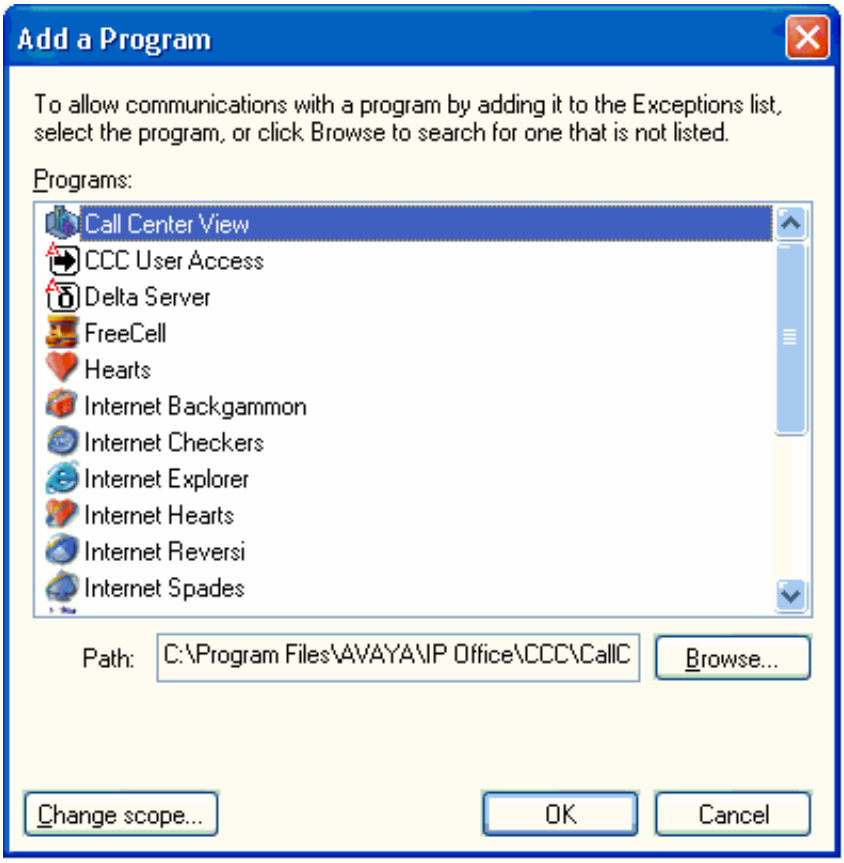
This will show the status of the firewall (default is on, with exceptions allowed, although none are configured at default. Higher settings may not allow the addition of exceptions). If the 'Don't allow exceptions' box is checked, then the modifications to the firewall to allow IP Office application will not be active.

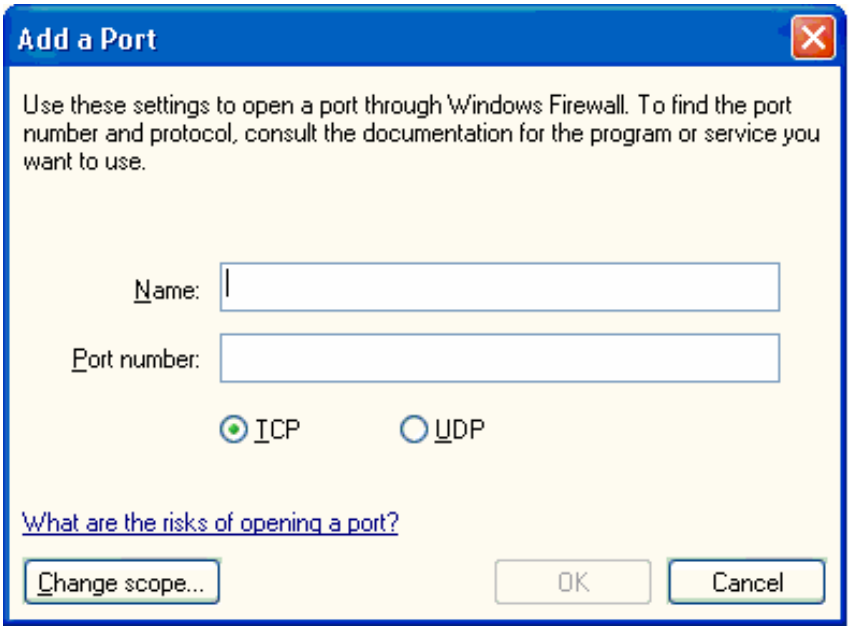


Select the Exceptions tab.

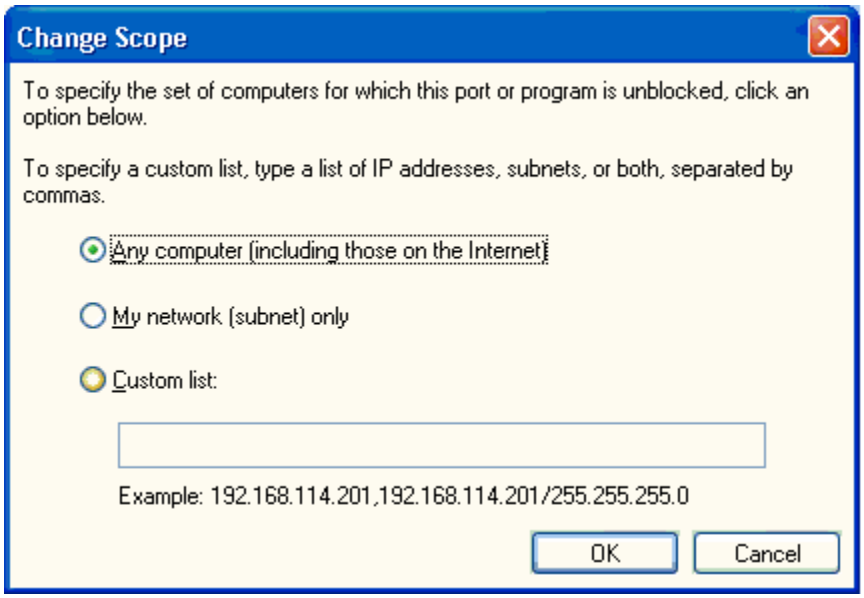


Click Add Program to select (or browse to a program) to add to the firewall, or Add Port to enter a port number and select TCP/UDP type. However, it is obviously more restrictive and thus safer, to just allow an application to have access, rather than a port.





Click on change scope to select the level of security required. Windows default is 'Any computer'.



The Advanced tab allows changes to the logging options, Services, and ICMP restrictions, should these be required.

Applications

The following applications have been tested for functional operation. This does not imply total compatibility, as additional modifications may be required to allow operation on a computer or network that does not have default security settings currently configured.

- Manager
- Upgrade Wizard
- Call Status
- Key Server
- System Monitor
- Voicemail Lite
- Phone Manager (Pro & Lite)
- Phone Manager VoIP client
- CCC multimedia MMS Client (Requires DCOM Modification)
- Integrated Messaging IMS Client for Outlook (Requires DCOM Modification)
- Soft Console
- Delta Server Service (V5)
- Delta Server Service Management Assistant (V5)
- Delta Server (V4)
- CBC

Further applications will be added to this list once their testing has been completed.

Security Levels

The Windows Firewall Exceptions can be specified to have one of three levels of security.

- Any Computer (including those on the Internet)
- My network (Subnet)
- Custom List

The more restrictive the scope, the safer the system will be from risk of attack. For this reason, Avaya recommend using the more restrictive scopes such as My network (subnet), or custom, with a limited IP range, rather than 'Any Computer'.

For simplicity the script file supplied with this document uses the 'Any Computer (including those on the Internet)' setting. The default can be changed in the attached batch file by editing the lines that include 'SCOPE=ALL' to read 'SCOPE=SUBNET' for enhanced security.
For higher security, this can be modified, by changing the scope parameter to custom list, to further enhance the security of the system. This will require knowledge of the system and the host network.

For example:-

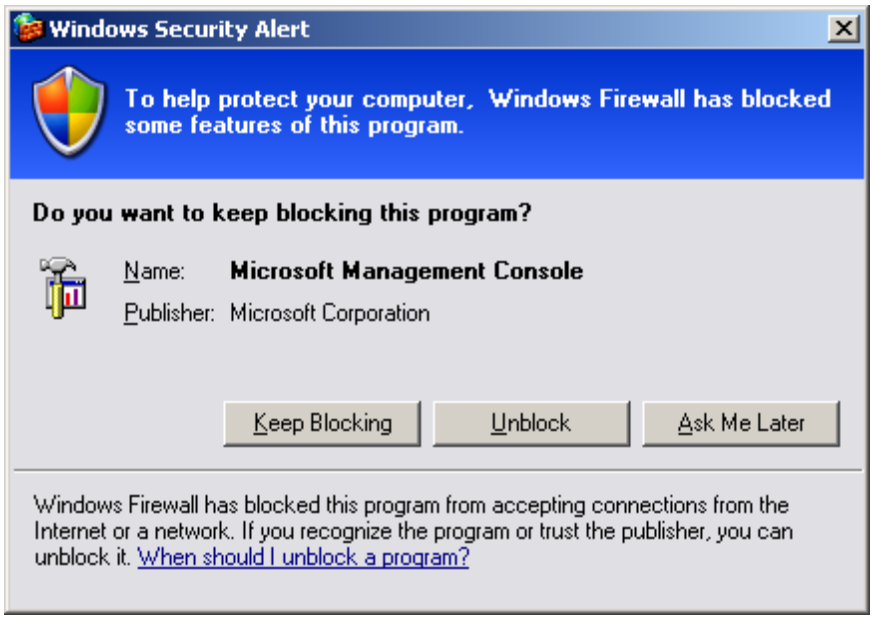
- Scope = ALL
- Scope = SUBNET
- Scope = CUSTOM Addresses = 192.168.42.0/24,LocalSubnet
    - Examples of addresses
        - 192.168.0.0/16 Address/mask length
        - 192.0.0.0/255.0.0.0 Address/mask
        - 192.168.42.44 Address
        - LocalSubnet Take local network range

Profiles can be configured to CURRENT, DOMAIN, STANDARD, or ALL

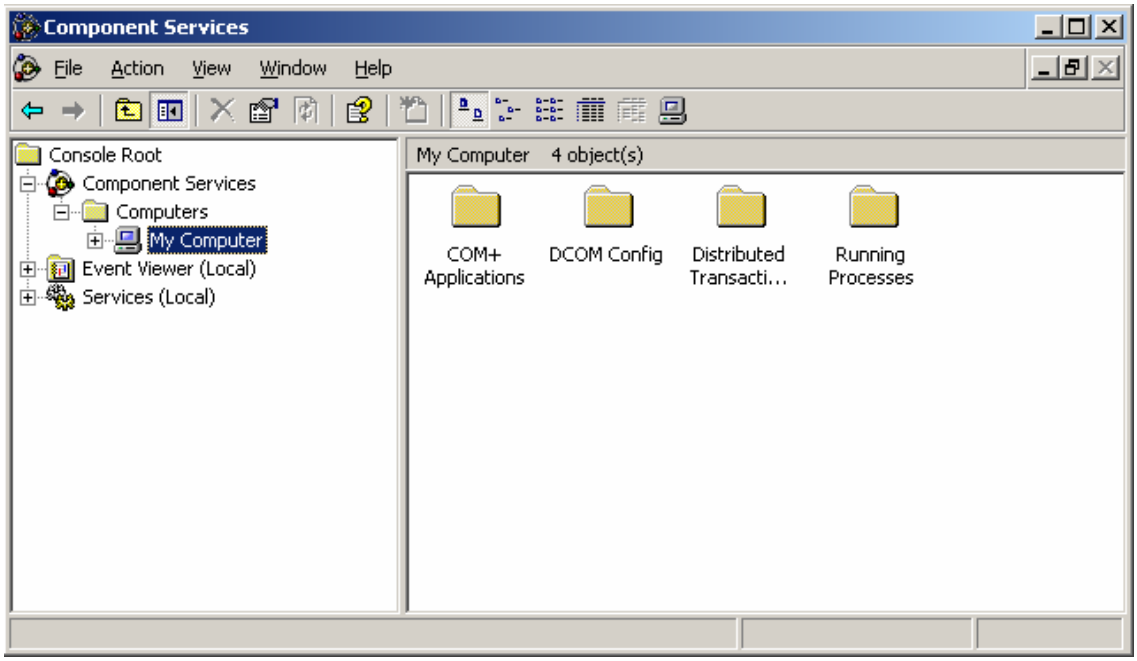
COM Objects Enhanced Security

Additional enhancements to the operating system, in the Windows XP Service Pack 2, are within the security of DCOM. This gives rise to applications failing to operate, without any clear indication of the failure.

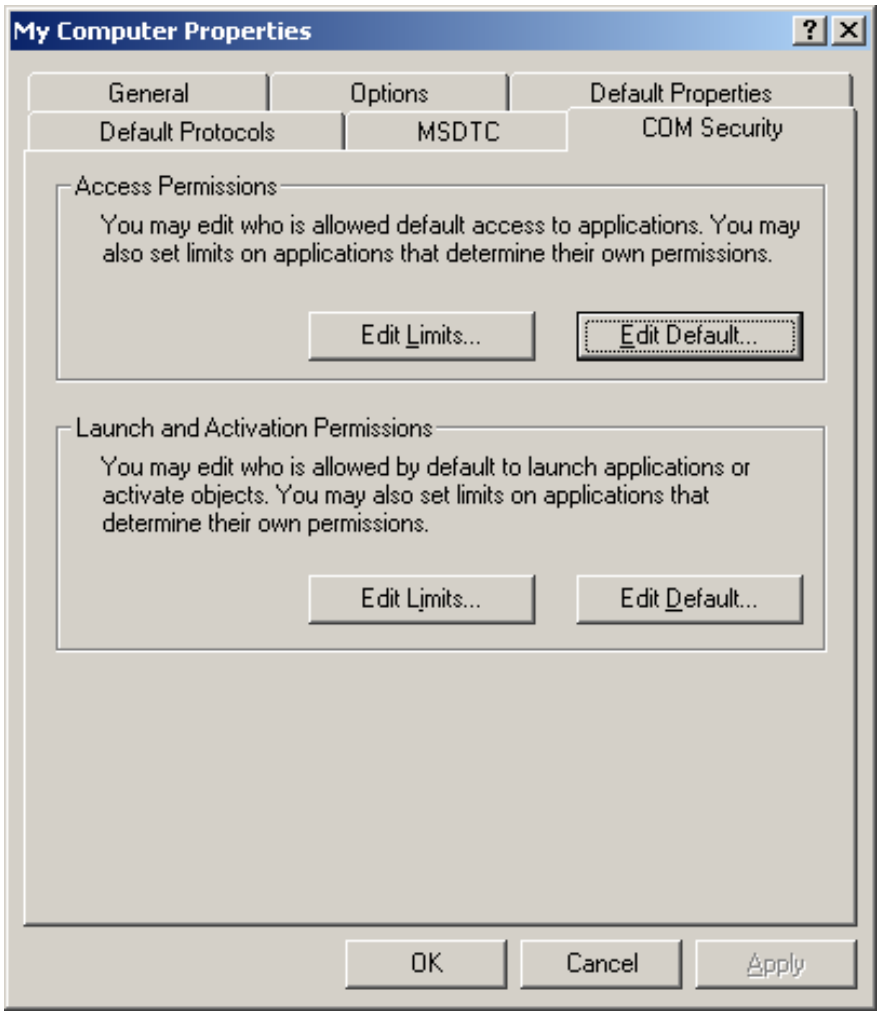
Within the IP Office application range there are programs, such as the IP Office IMS client, which utilise DCOM. The following information shows how to modify the security level to enable their correct operation. When running the component services icon (from Administration) or 'dcomcnfg' from the command line for the first time after the service pack installation, you will receive a security alert.



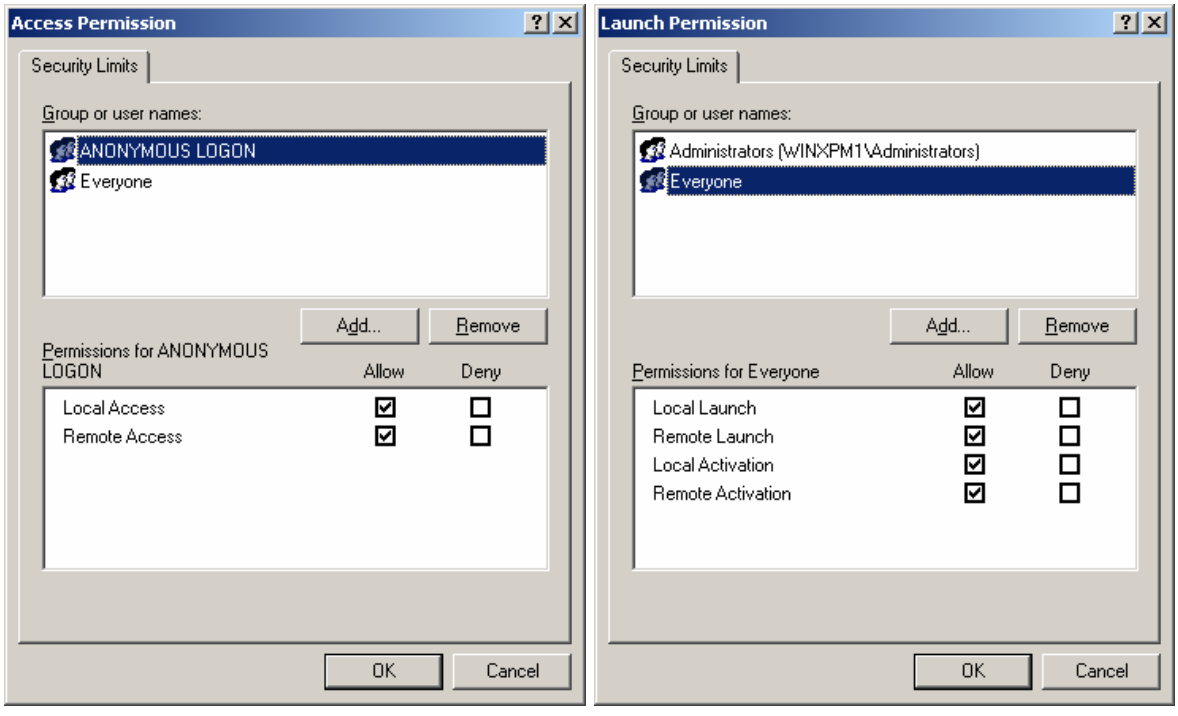
Select ‘Unblock’ to continue. Navigate down to ‘My Computer’ and select properties.



Select the COM Security tab.



Now edit the limits for ‘Access Permissions’ and ‘Launch and Activation Permissions’ to allow Remote Access and remote Launch/Activation permissions for anonymous and everyone.



After changing, click OK, and close Component Services manager.

Enhancing Security Settings

This document, and the script file listed, makes no assumption about the construction of the network that the IP Office and associated software is being used on. By having knowledge of this, it is possible to increase the security by narrowing the scope of the firewall exceptions. The security level section shows the levels available.

Consider the following scenario

Small Community Network
IP Office IP 172.16.4.1
Mask 255.255.255.0

Computers located on local subnet. External access is through IP Office.

For this scenario, the scope parameter within the script file could be changed from *'scope=ALL'* to *'scope=SUBNET'* to increase the security of the Windows firewall. This can also be changed through the Windows Firewall Applet from the control panel.

Consider the second scenario

Wide Area Network
IP Office 1 192.168.42.1
Mask 255.255.255.0
IP Office 2 192.168.43.1
Mask 255.255.255.0
IP Office 3 192.168.44.1
Mask 255.255.255.0

For a computer located on the first LAN 192.168.42.0, setting the scope to only include the subnet, would inhibit working with the other IP Office units. It is possible to limit the scope of the firewall in different ways using the custom option.

The three examples are listed below (note that even the lowest level security example here is far greater than that supplied by the default scope option)

- Scope=custom address=localsubnet, 192.168.43.1, 192.168.44.1
    - Highest security level. Only the local subnet, and the specific addresses outside of the local subnet are allowed through the firewall
- Scope=custom address=localsubnet, 192.168.43.0/24, 192.168.44.0/24
- Scope=custom address=192.168.0.0/16
    - Lowest level custom scope. Any unit through out the networks 192.168.1.1 to 192.168.255.1 are excepted through the firewall

- ***Appendix A – AvayaFW.bat***

The file attached below is a sample batch file containing the relevant firewall exceptions for the Avaya IP Office applications.

To SAVE this file to your computer
To save this file to your computer for distribution to other computers or to run later:
right-click on the paperclip icon, then select ‘Save Embedded File to Disk’.

> *NOTE: Please note that double-clicking on this file once it has been saved to your computer will cause the script to run. Should you wish to examine the contents of the script, right-click the file and select ‘Edit’.*

To RUN this file on your computer
To run this file now directly from this document:
right-click on the paperclip icon, then select ‘Open File’.

Issued by:
Avaya SMBS Tier 4 Support
Tel: +44 (0) 1707 392200
Fax: +44 (0) 1707 376933
Website: www.avaya.com
Email: gssfsg@avaya.com