



IP Office Technical Tip

Tip no: 113

Release Date: 4 November 2005

Region: GLOBAL

Windows 2003 SP1 Security Modifications for Avaya IP Office Voicemail Pro and Avaya IP Office Manager

This document outlines changes to the configuration of Windows 2003 Server SP1 that are required to run IP Office Manager and IP Office VoiceMail Pro. Microsoft has introduced a set of security technologies in Server 2003 Service Pack 1 that improves the ability of computers running Windows Server 2003 to withstand attacks from viruses and worms. Changes have been made to DCOM, Windows Firewall and various integrated components. Microsoft has also introduced a new tool to help manage security policy called the Security Configuration Wizard (SCW).

Microsoft has published a white paper that reviews Server 2003 SP1 functionality changes. Additional information on this subject can be found using the following link:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=C3C26254-8CE3-46E2-B1B6-3659B92B2CDE&displaylang=en>

The security policy enforced by Service Pack 1 requires modifications in order for IP Office applications to work properly and maintain functionality. The following procedure documents the modifications needed for IP Office Voicemail Pro and IP Office Manager to function correctly.

Security Configuration Wizard Installation

Click Settings/Control panel/Add or remove programs, then select add/remove windows components.

Scroll down the list to select and install the "Security Configuration Wizard".

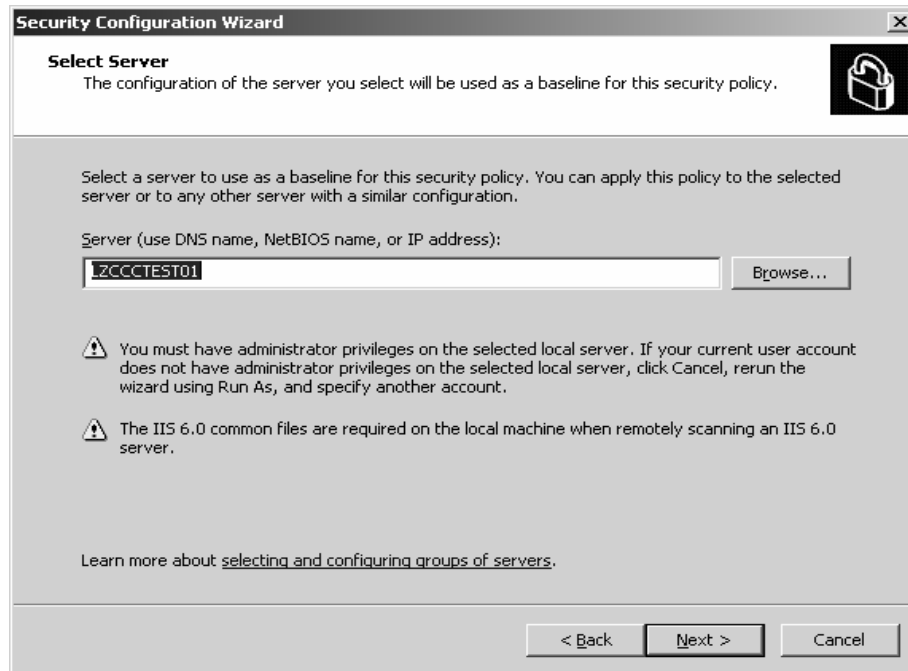
Once installed, to launch the SCW, click Start, then Run, and type scw (scw.exe) or select Control Panel/Administrative tools/Security Configuration Wizard.



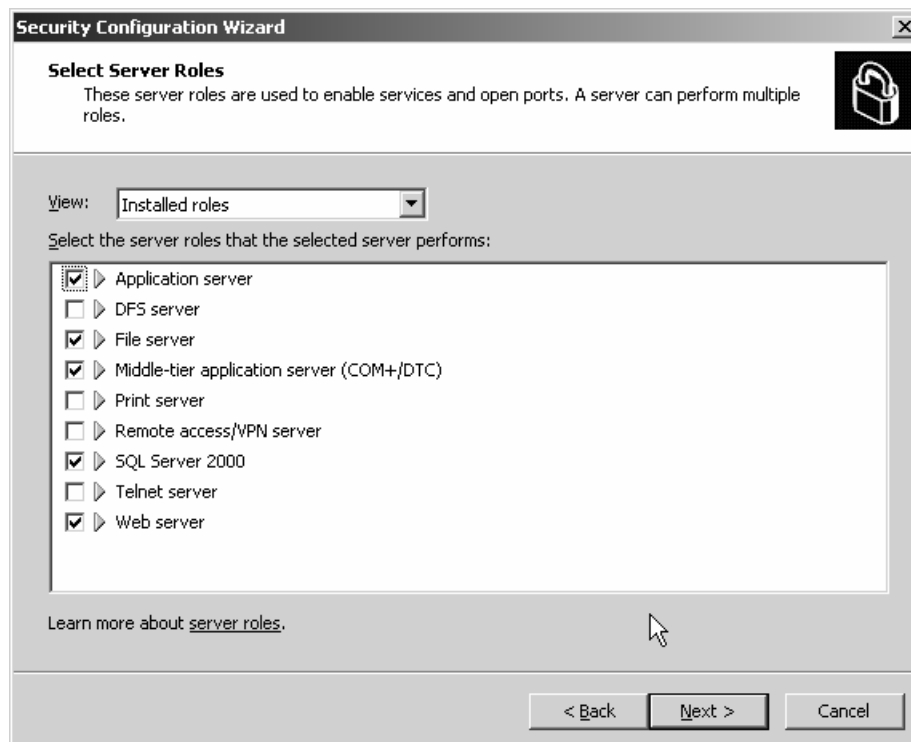
At the welcome screen, click 'Next' to start the Security Configuration Wizard.



Select "Create a new security policy" then click 'Next' to proceed.

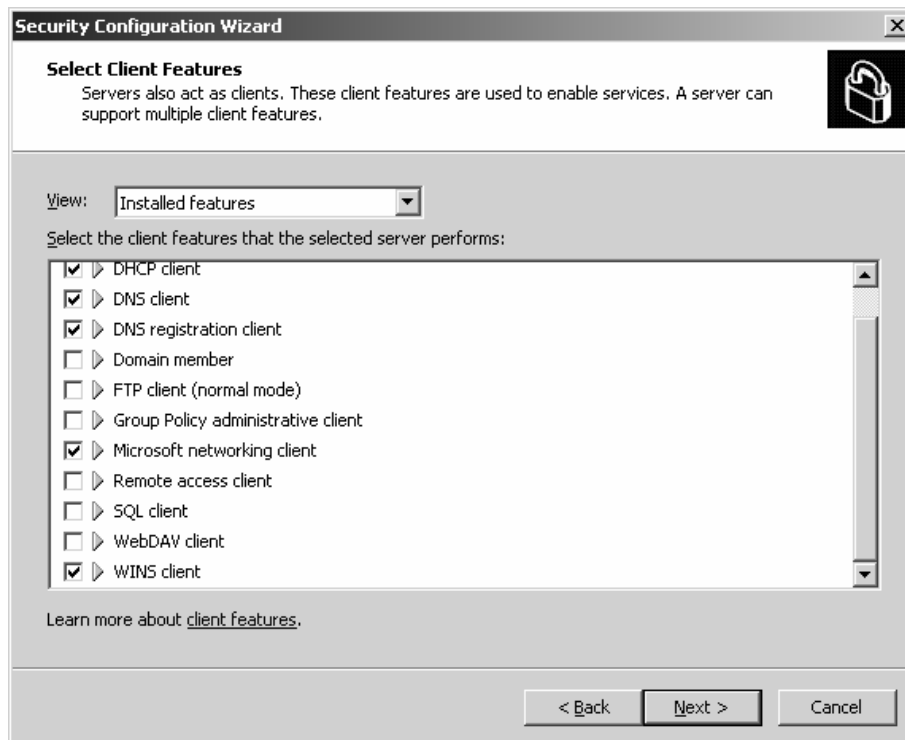


Leave the hostname if it is populated correctly, then click Next (there will be a short pause), when complete click Next. If the hostname is incorrect, click 'Browse' to search for the correct Server.

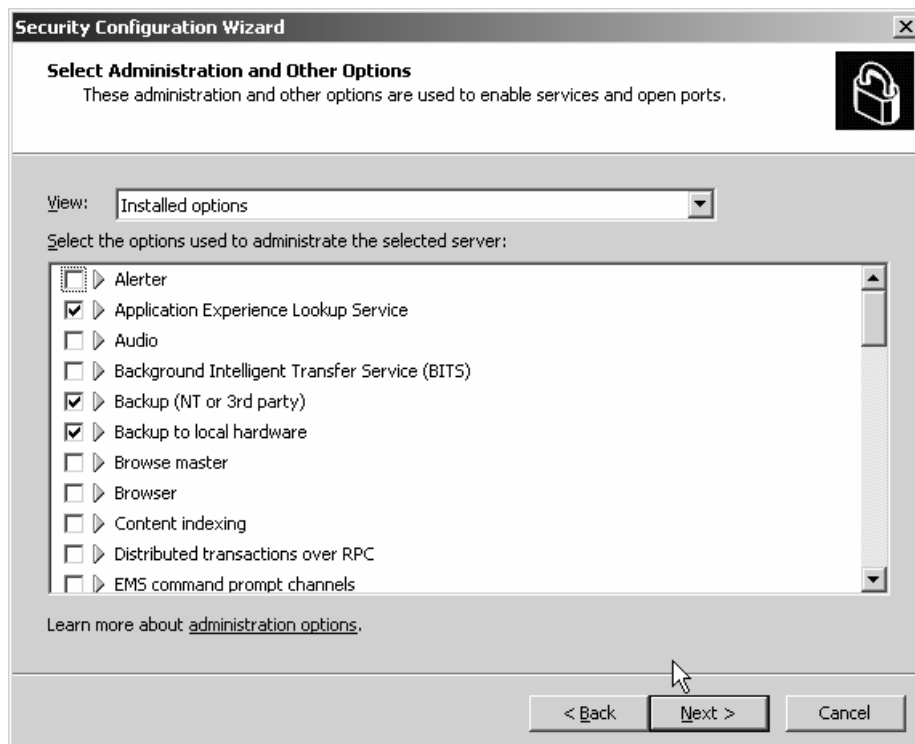


The Select Server Roles defaults should be correct, these should be reviewed and corrected if necessary before selecting 'Next' to proceed. In the example above, SQL

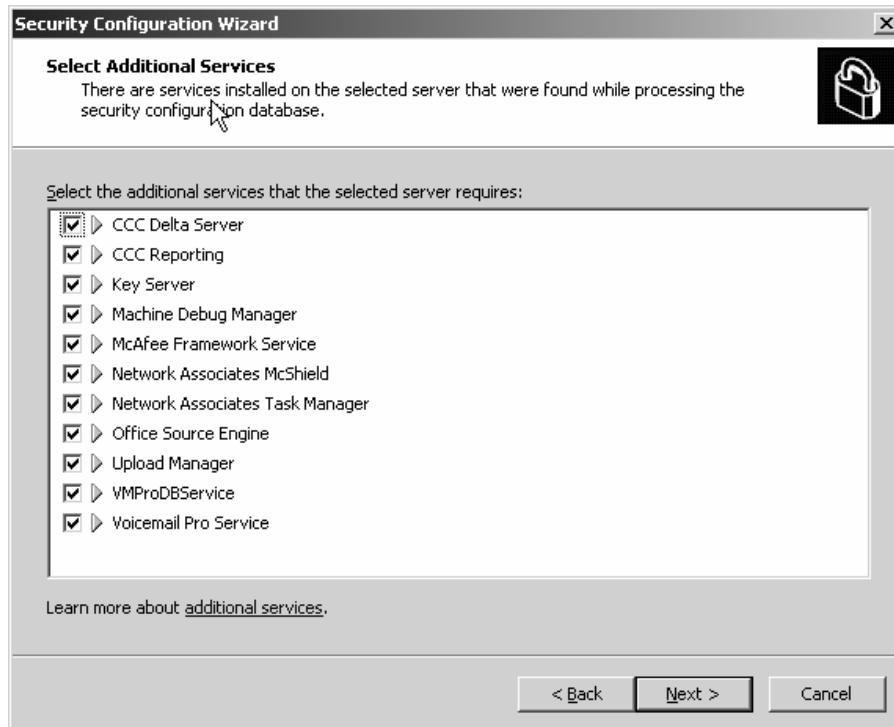
Server 2000 has been installed in order to run Compact Contact Center.



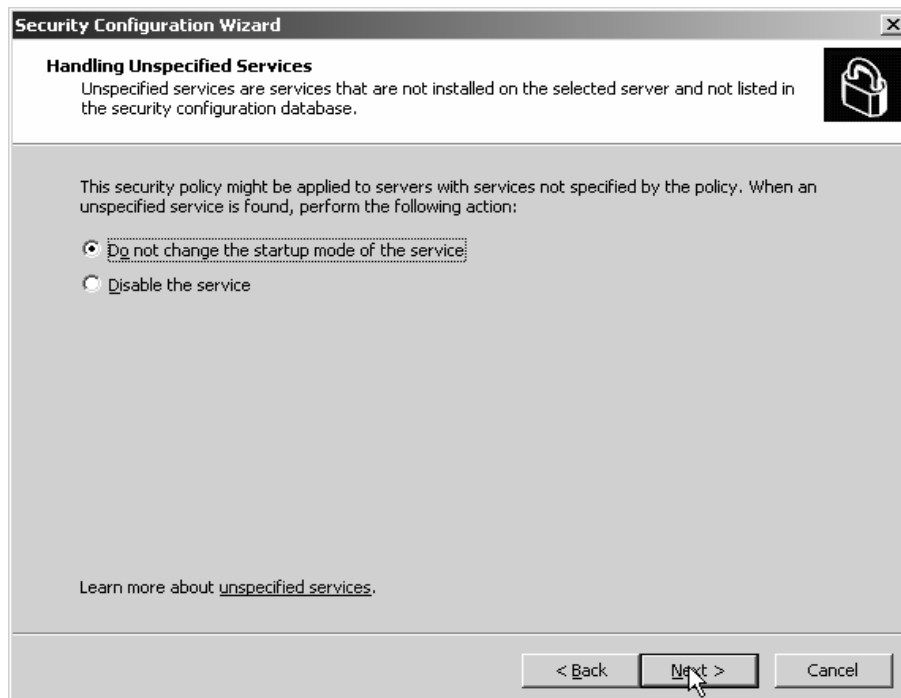
The default 'Installed Features' should be correct for the 'Select Client Features' page, but should be reviewed and amended if necessary before selecting 'Next' to proceed.



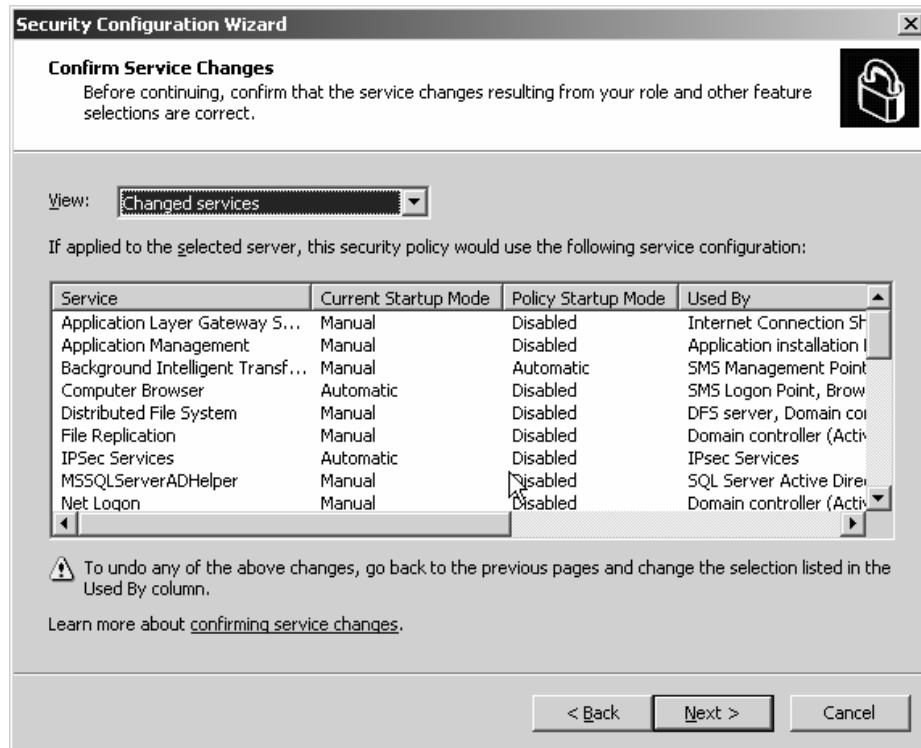
The default 'Installed options' should be accepted by selecting 'Next'.



IMPORTANT – Confirm that all IP Office Applications have been checked before selecting 'Next' to continue.



IMPORTANT – ‘Do not change the startup mode of the service’ MUST be selected before clicking ‘Next’ to proceed.



Security Configuration Wizard

Confirm Service Changes
Before continuing, confirm that the service changes resulting from your role and other feature selections are correct.

View: **Changed services**

If applied to the selected server, this security policy would use the following service configuration:

Service	Current Startup Mode	Policy Startup Mode	Used By
Application Layer Gateway S...	Manual	Disabled	Internet Connection SH
Application Management	Manual	Disabled	Application installation I
Background Intelligent Transf...	Manual	Automatic	SMS Management Point
Computer Browser	Automatic	Disabled	SMS Logon Point, Brow
Distributed File System	Manual	Disabled	DFS server, Domain coi
File Replication	Manual	Disabled	Domain controller (Activ
IPSec Services	Automatic	Disabled	IPsec Services
MSSQLServerADHelper	Manual	Disabled	SQL Server Active Dire
Net Logon	Manual	Disabled	Domain controller (Activ

⚠ To undo any of the above changes, go back to the previous pages and change the selection listed in the Used By column.

Learn more about [confirming service changes](#).

< Back Next > Cancel

Review the changes made in the steps above, going back if necessary to correct the changes, before selecting ‘Next’ to proceed.



Security Configuration Wizard

Network Security

Use this section to configure inbound ports using Windows Firewall based on the roles and administration options that you selected. In addition, you can restrict access to ports and indicate if port traffic is signed or encrypted using Internet Protocol Security (IPsec).

⚠ Answering these questions incorrectly might prevent the selected server from communicating with other computers.

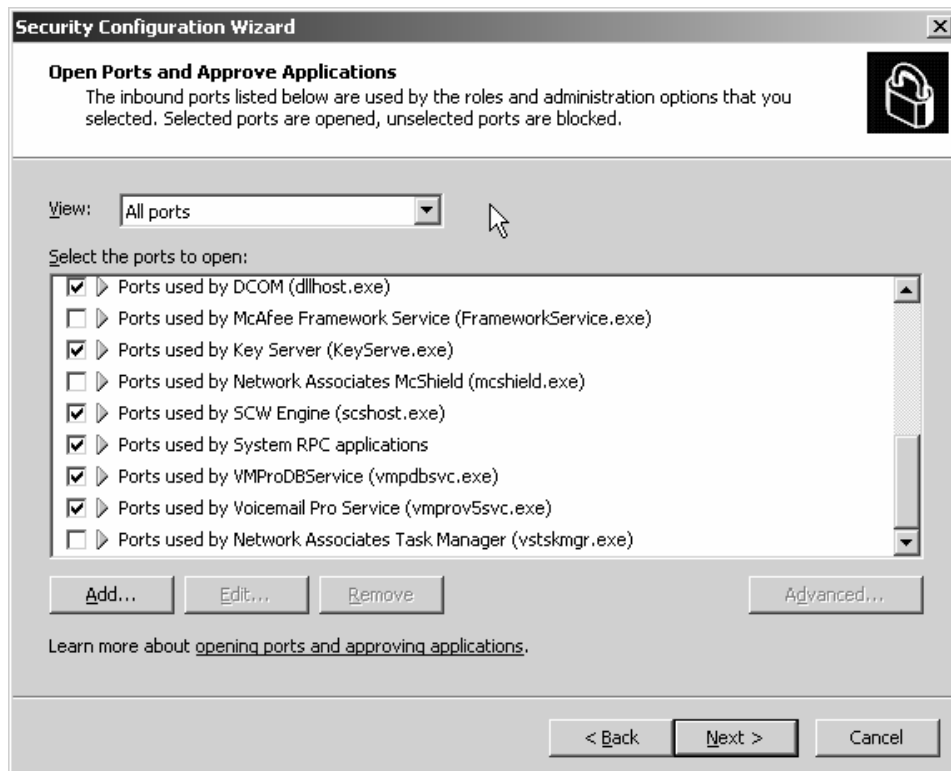
☐ **Skip this section**

If you skip this section, this security policy will not configure Windows Firewall or IPsec settings. If you do not skip this section, Windows Firewall will be enabled, and IPsec may be enabled as necessary, to support configuration and use of the firewall.

Learn more about [network security](#).

< Back Next > Cancel

Do not select 'Skip this section', then click 'Next' to proceed.



Review the list provided, and confirm that all IP Office applications installed are selected, before clicking 'Next' to continue.

Notice ports used by IP Office Applications:-

VoiceMail Pro Database Service –

Ports used by VMProDBService (vmpdbsvc.exe)

Description: SCW discovered the VMProDBService application listening on the following ports: 8085/TCP. If you select this option, all ports used by the application will be opened automatically by Windows Firewall

Path: C:\Program Files\Avaya\IP Office\Voicemail Pro\VM

Used by: VMProDBService

VoiceMail Pro Service –

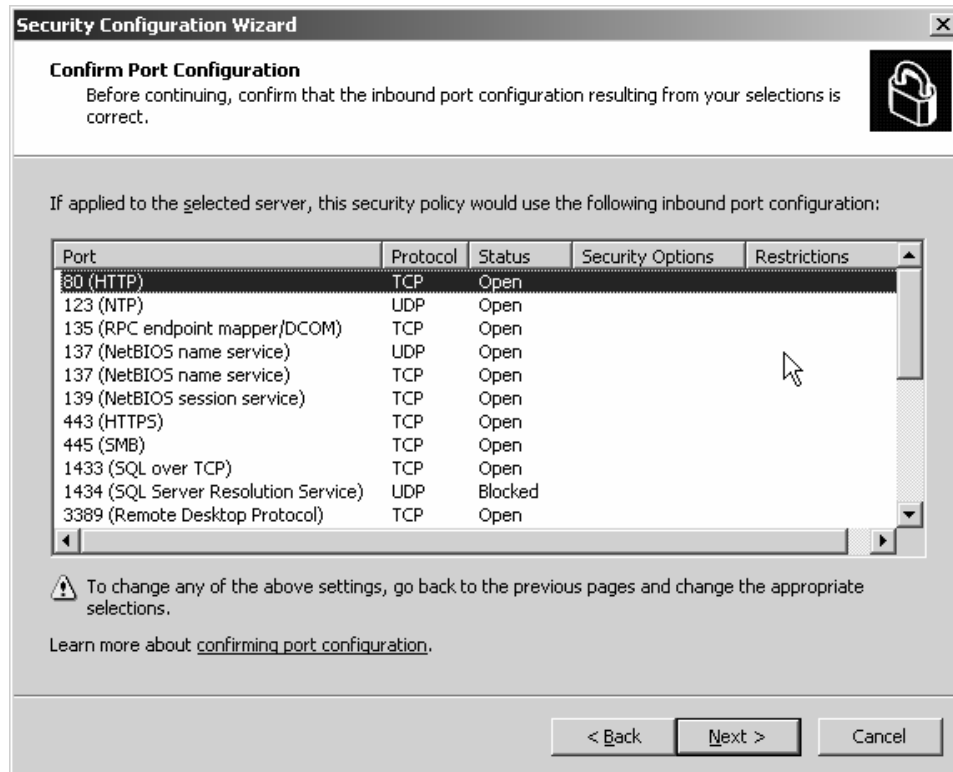
Ports used by Voicemail Pro Service (vmprov5svc.exe)

Description: SCW discovered the VoicemailProServer application listening on the following ports: 50791/UDP, 37/UDP. If you select this option, all ports used by the application will be opened automatically by Windows Firewall

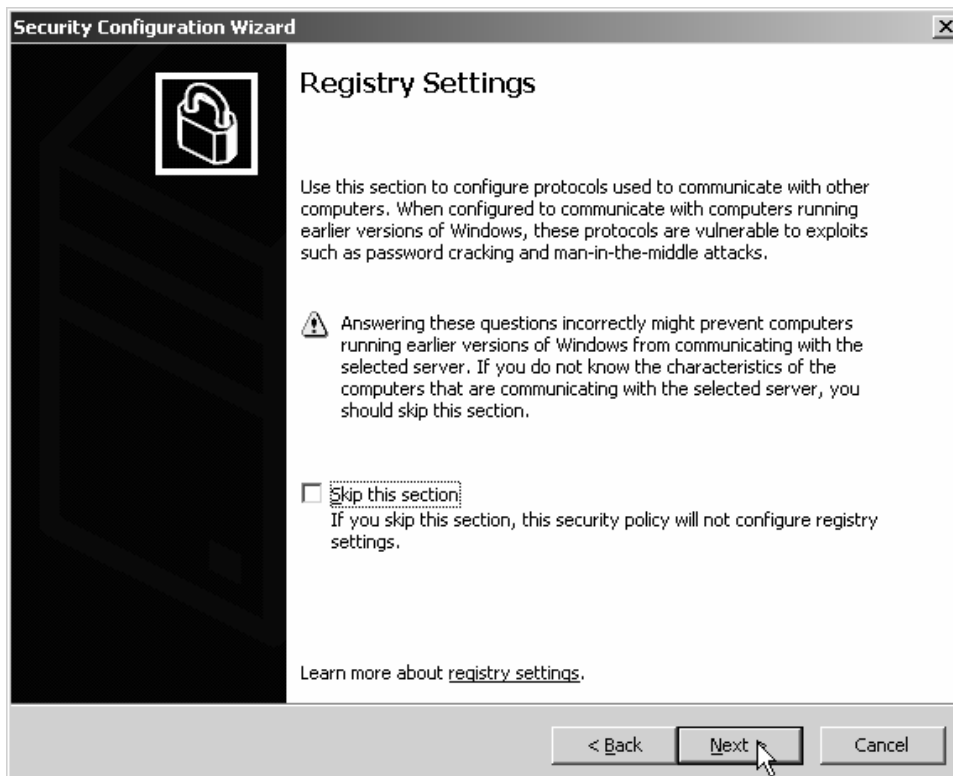
Path: C:\Program Files\Avaya\IP Office\Voicemail Pro\VM

Used by: Voicemail Pro Service

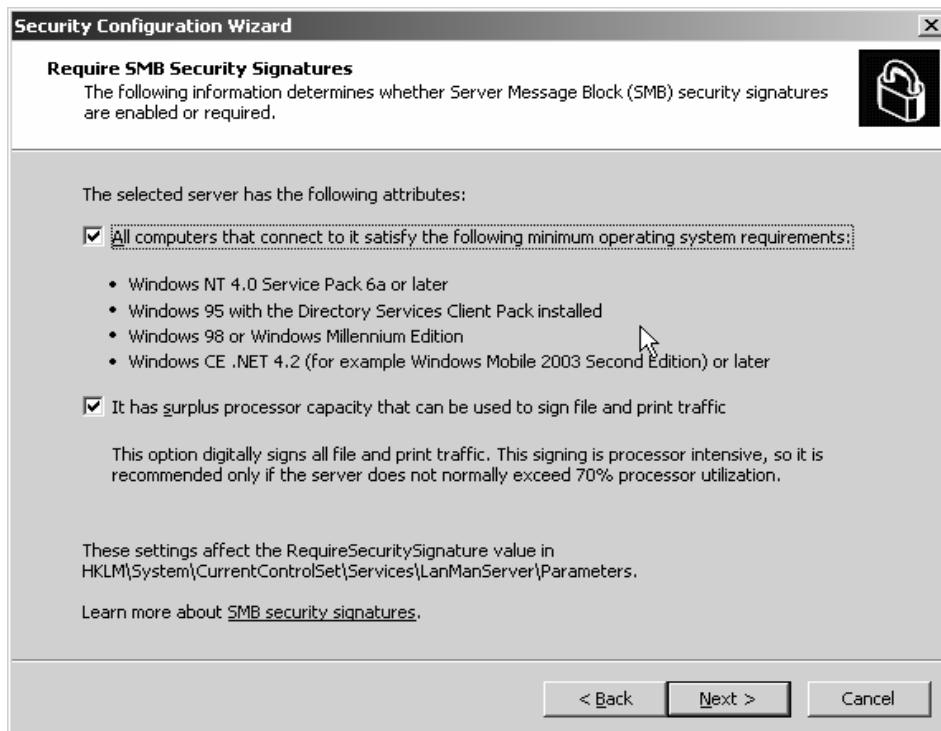
NOTE – the IP Office Manager application will be added to firewall exclusion list in a later step.



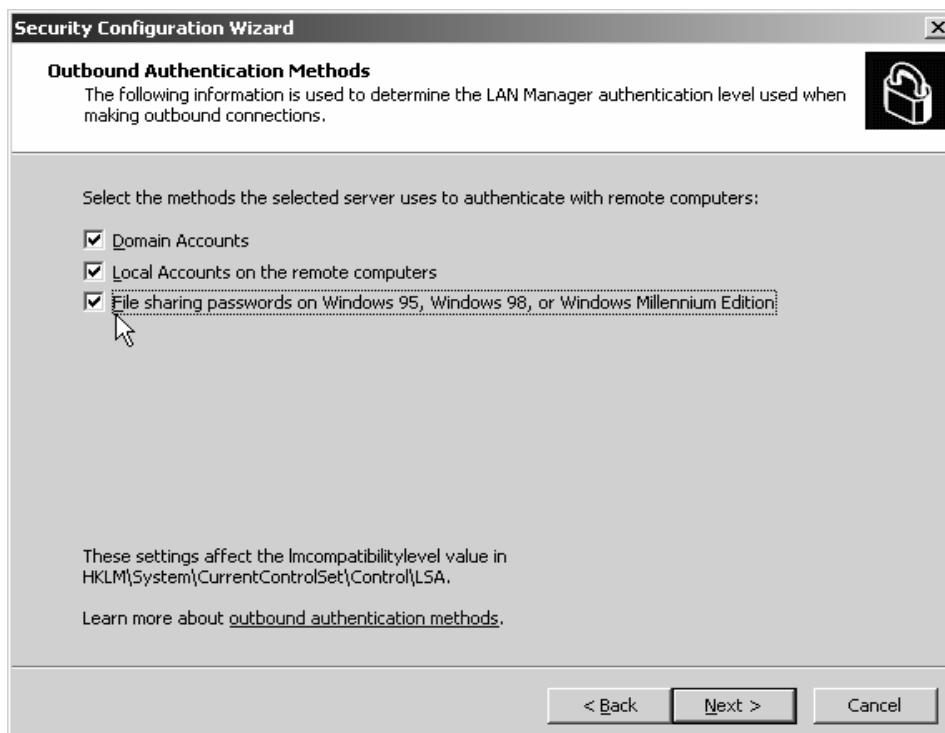
Take time to review the selected ports, then select 'Next' to continue.



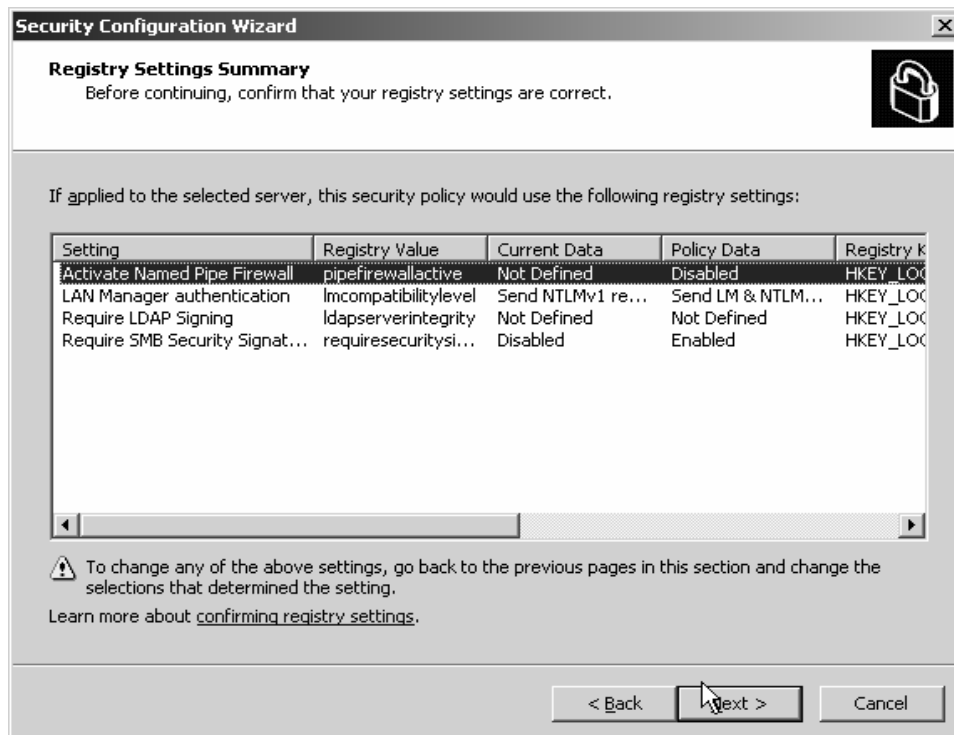
Do not select 'Skip this section', then click 'Next' to proceed.



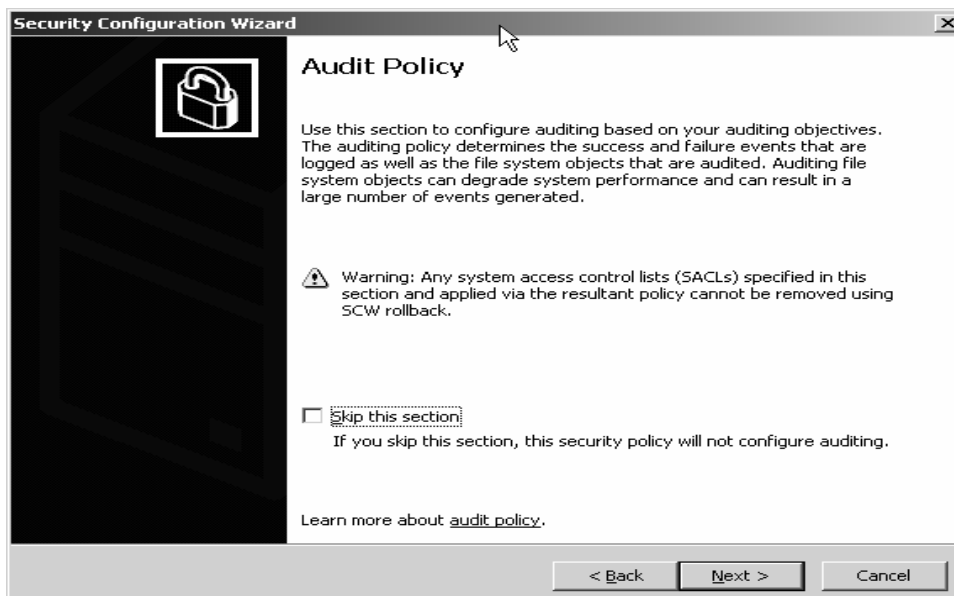
Leave the selections as default to ensure multiple Operating System compatibility then select 'Next' to continue.



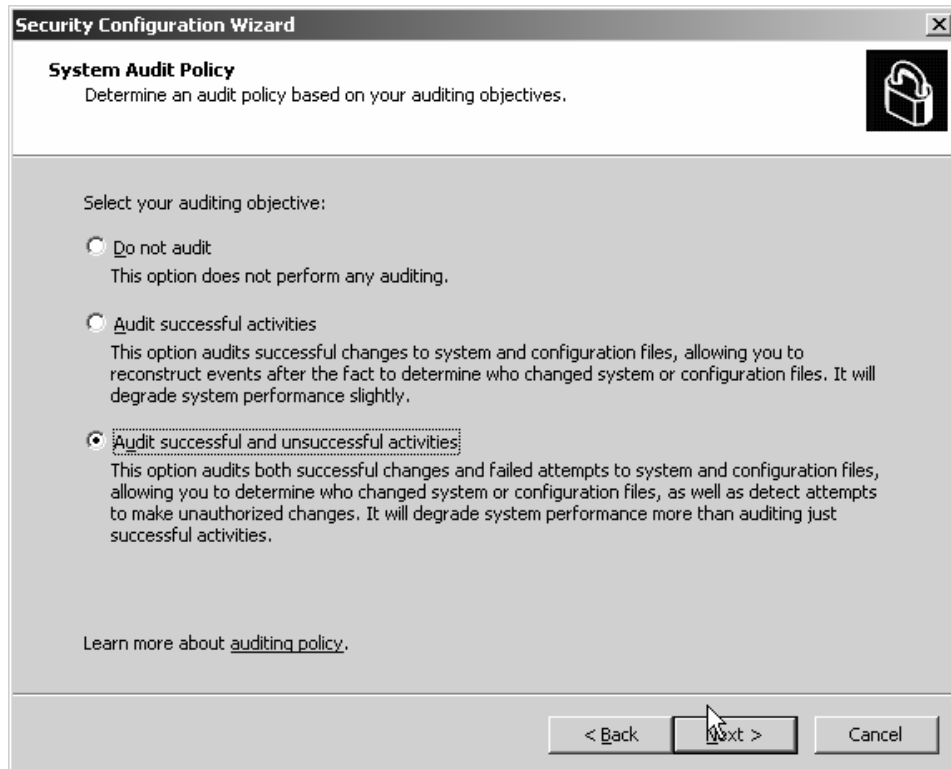
Check all authentication methods for maximum compatibility, then select 'Next' to continue.



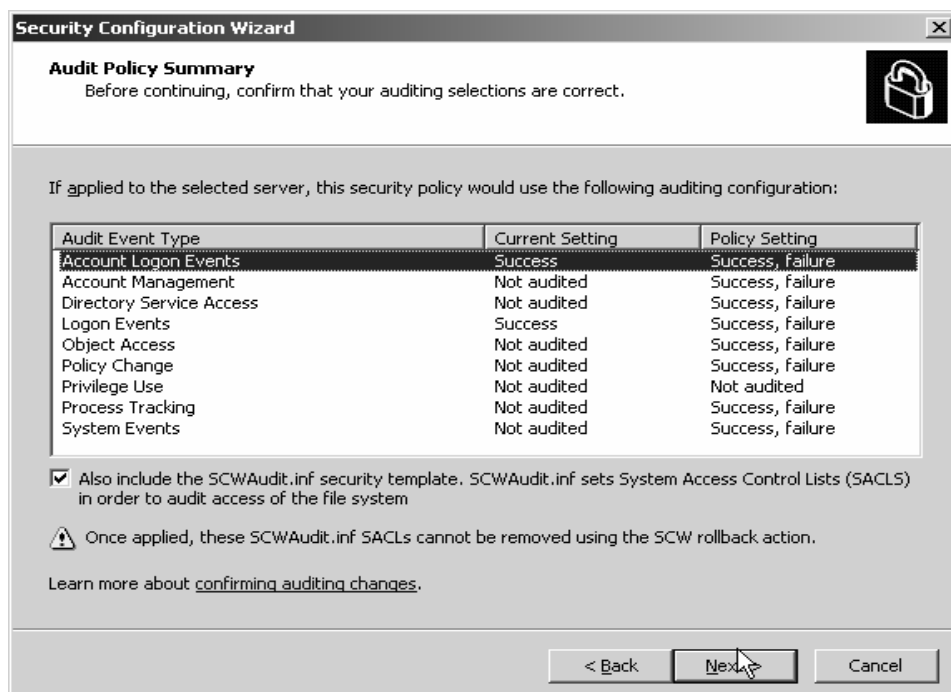
Review the changes you have made, then select 'Next' to continue.



Do not select 'Skip this section', then click 'Next' to proceed.



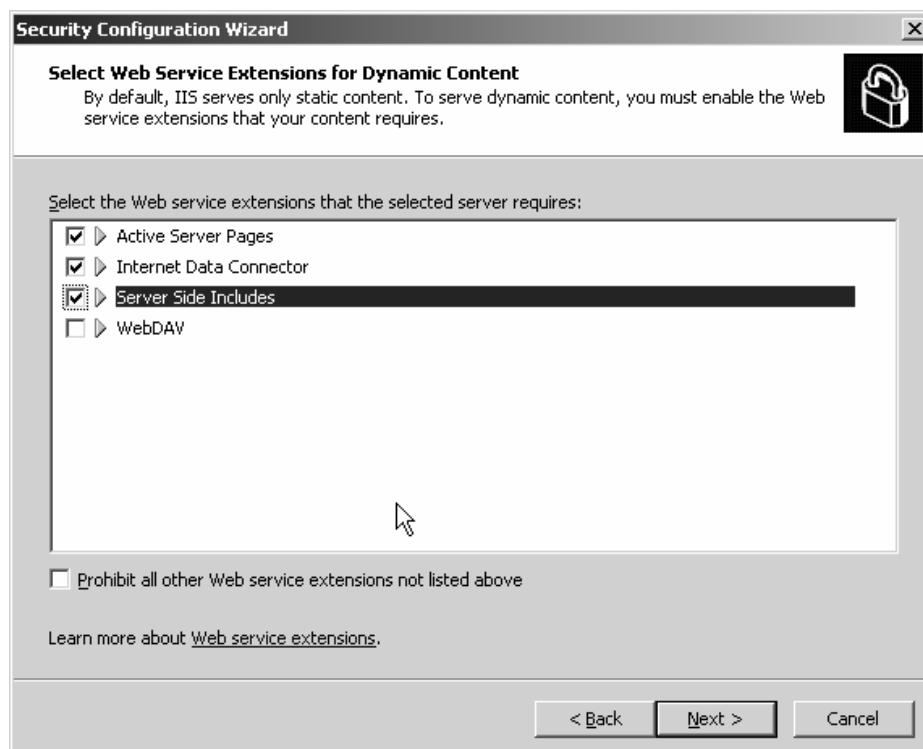
Select an audit policy according to organizational preferences, then select 'Next' to continue.



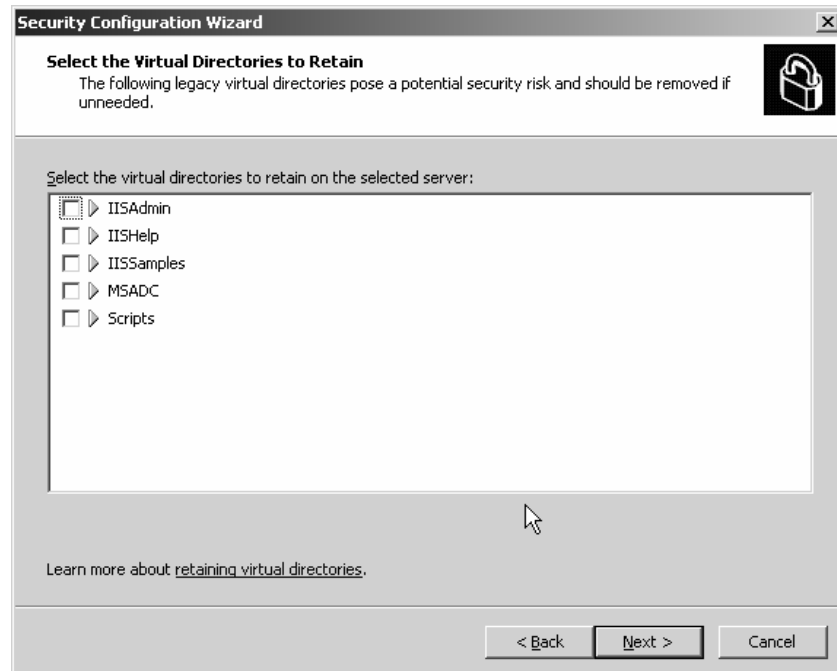
Review and confirm the selected audit policy by selecting 'Next'.



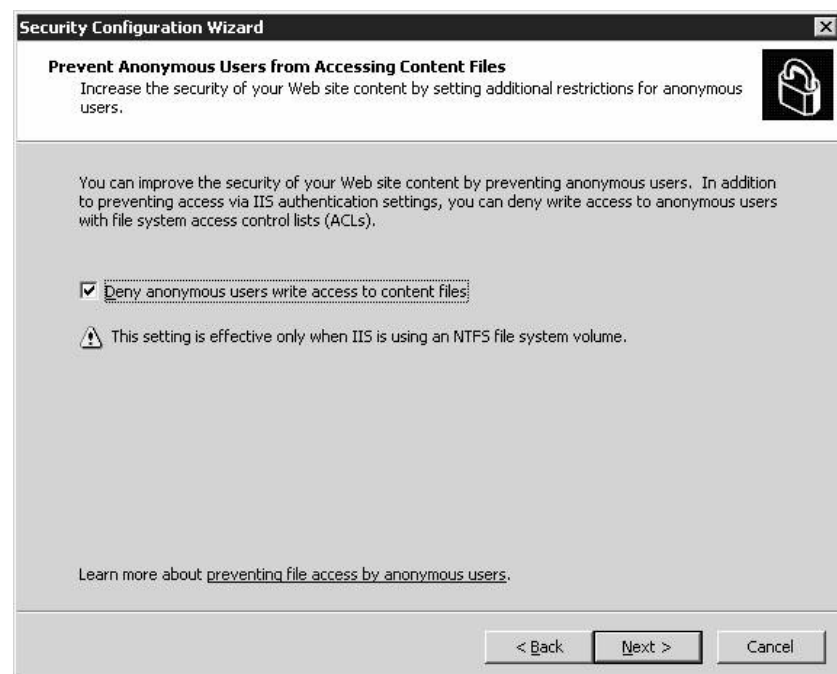
Do not select 'Skip this section', then click 'Next' to proceed.



Select the options for supported Web service extensions based on current and future needs, then select 'Next' to continue

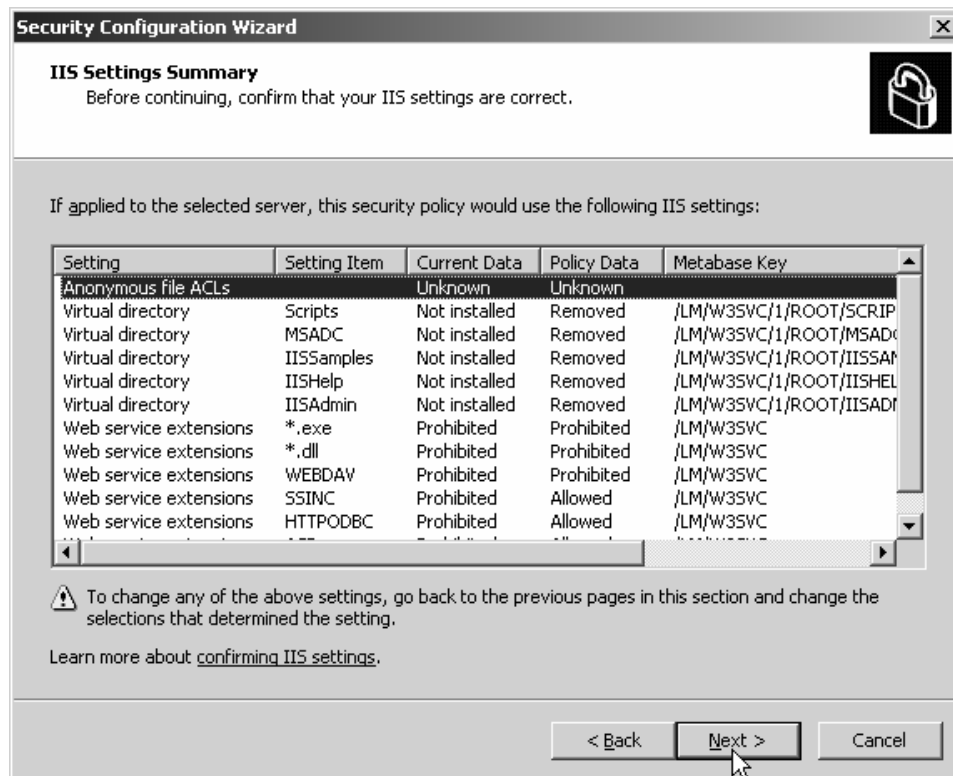


None of these directories are required by IP Office applications and can be left unselected unless otherwise required by alternate applications. Select 'Next' to continue.



This can be left un-checked to allow anonymous access if desired, or selected to increase security (recommended) if the web server is to be made available for external

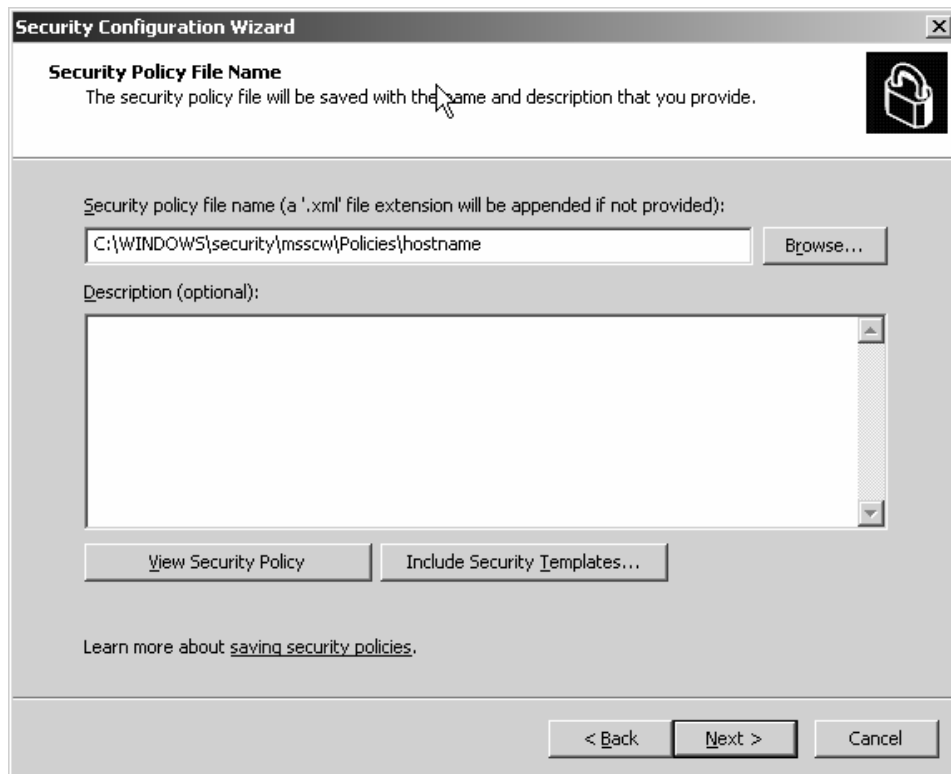
access. Select 'Next' to continue.



Review and verify the IIS settings then select 'Next' to continue.



Select 'Next' to save the security policy that has been created by the Wizard.



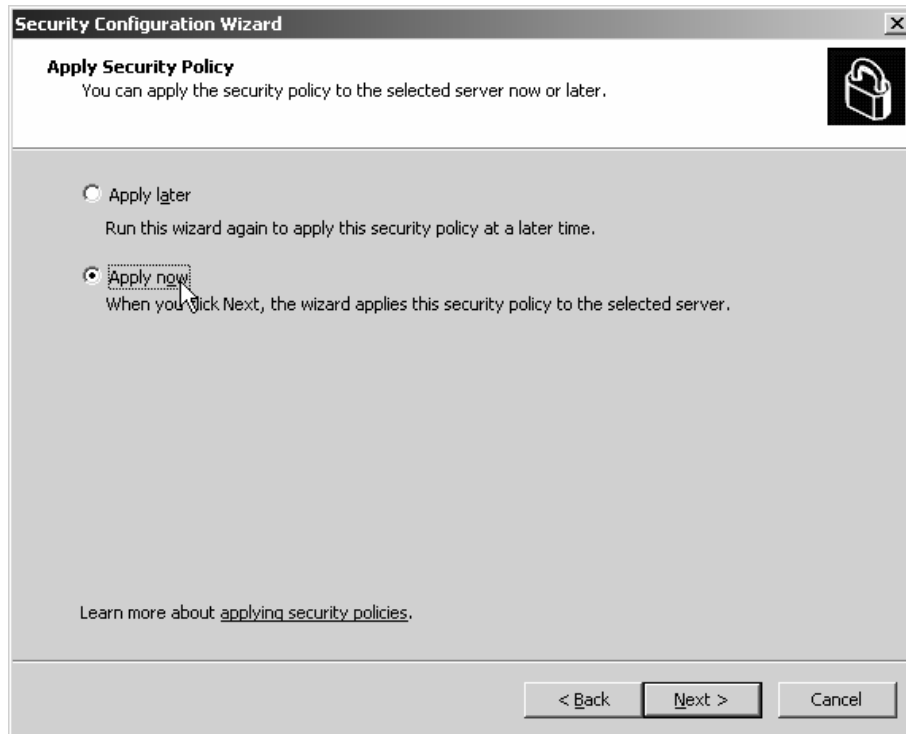
The image shows the 'Security Configuration Wizard' dialog box. The title bar reads 'Security Configuration Wizard'. The main heading is 'Security Policy File Name'. Below it, a message states: 'The security policy file will be saved with the name and description that you provide.' To the right of this message is a small icon of a padlock. Below the message, there is a text input field for the 'Security policy file name (a '.xml' file extension will be appended if not provided):'. The field contains the text 'C:\WINDOWS\security\msscwl\Policies\hostname'. To the right of the field is a 'Browse...' button. Below the field is a text area for the 'Description (optional):'. At the bottom of the dialog, there are two buttons: 'View Security Policy' and 'Include Security Templates...'. Below these buttons is a link that says 'Learn more about [saving security policies](#).' At the very bottom of the dialog, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Enter a filename (the PC's hostname) to replace 'hostname', then select 'Next' to continue.

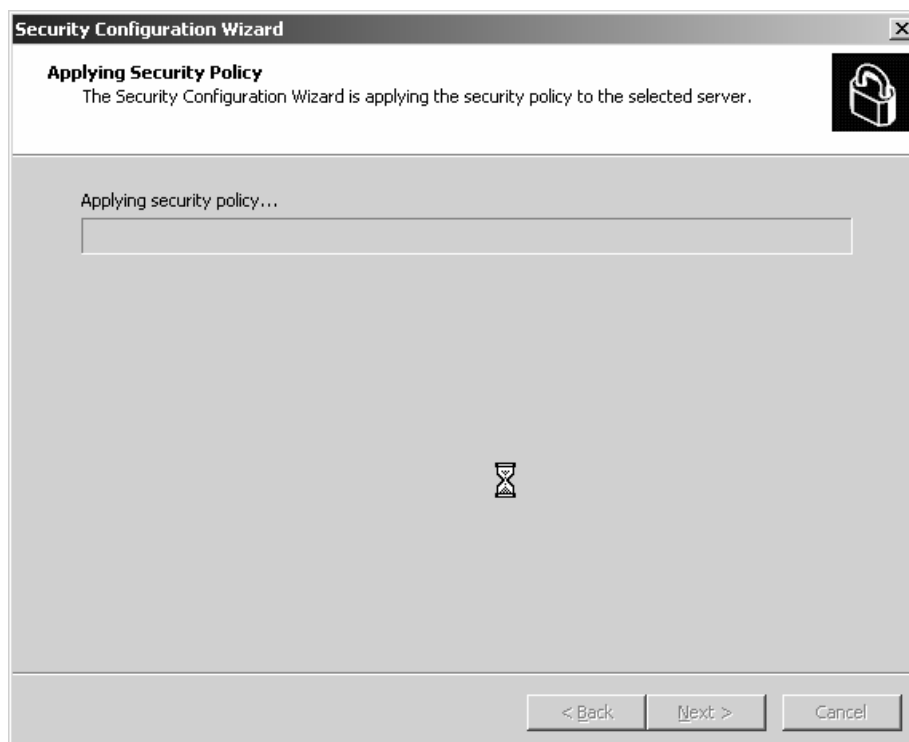


The image shows a warning dialog box from the 'Security Configuration Wizard'. The title bar reads 'Security Configuration Wizard'. On the left side, there is a warning icon (a triangle with an exclamation mark). To the right of the icon, the text reads: 'Applying this security policy to the selected server will require a reboot after the policy is applied. This is required for the configured applications or services to run properly.' At the bottom center of the dialog, there is an 'OK' button.

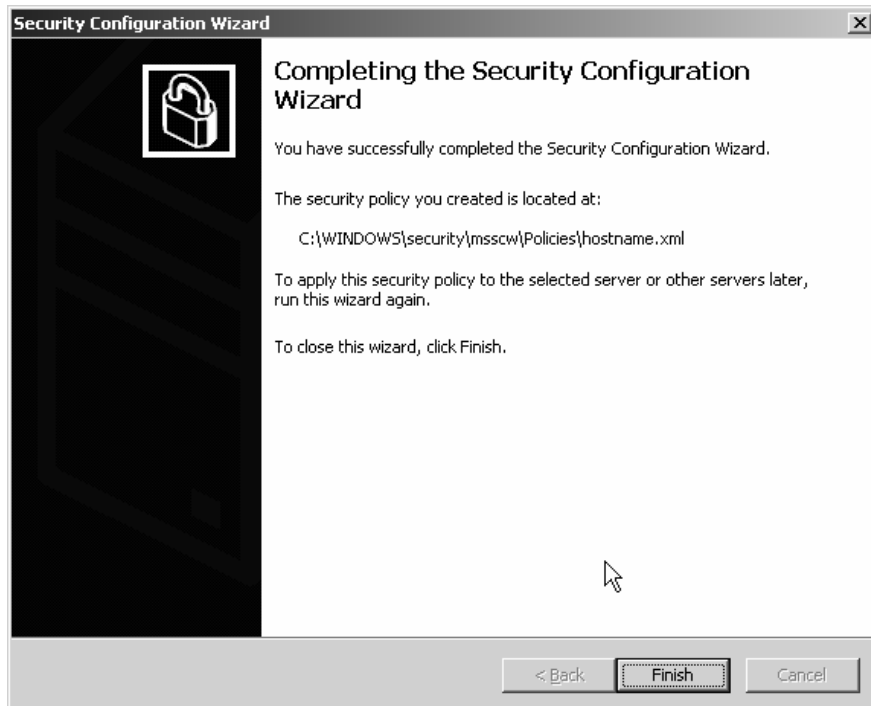
Select 'OK' to continue at the Security Configuration Wizard warning message.



Select 'Apply now', then 'Next' to make the policy active.



The Wizard will now apply policy. This may take a few minutes. Select 'Next' when complete.



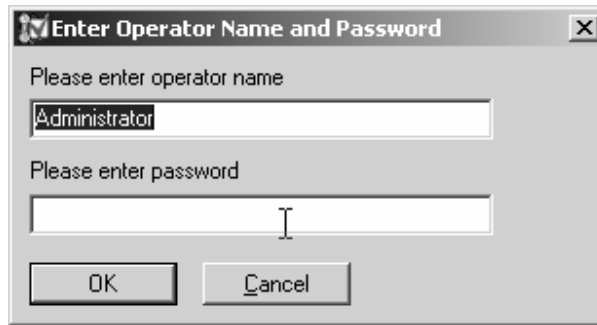
Select 'Finish' to exit the Security Configuration Wizard. A reboot is not prompted for at this point, but is required for some aspects of the security policy to be implemented. If the policy needs reviewing or amending, the Security Configuration Wizard can be run again, and the option to edit a previously saved policy selected.

After rebooting the server, run the IP Office manager application.

This warning will display:

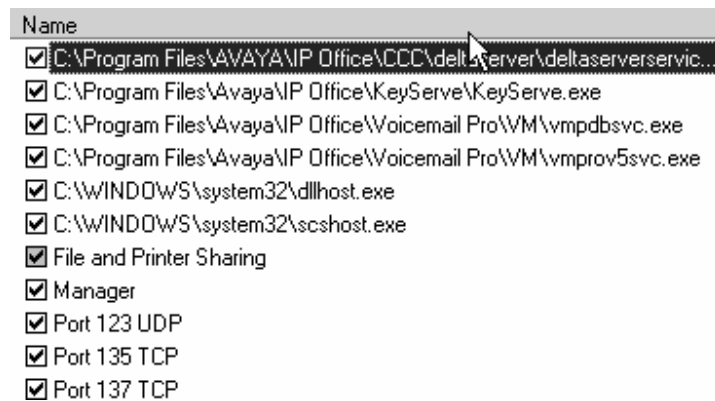


Select Unblock to allow the IP Office Manager application to function correctly, then Login as normal:



The windows firewall has now been updated with an “exception” for the IP Office Manager application.

To confirm this, open ‘My Network Places’, select the ‘Local Area Connection’, then right click on this connection to display the properties dialog. Select the advanced tab, then ‘Settings’ to display the Windows Firewall settings:



Notice that the IP Office applications are present in the list –“manager” is the IP Office Manager application.

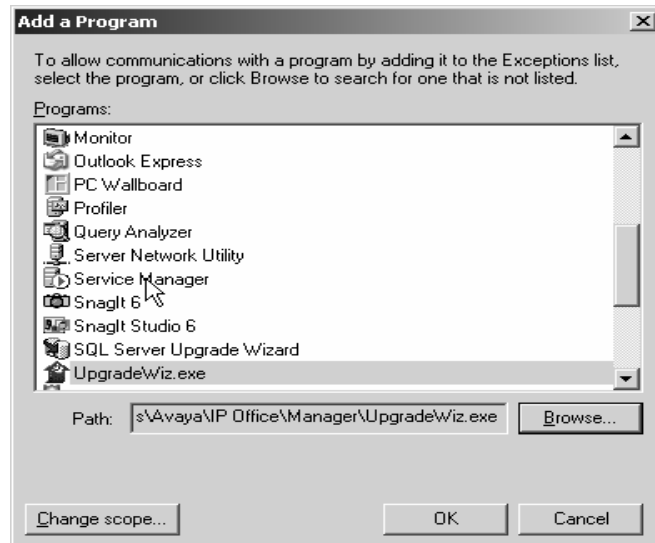
An exception is also required for the IP Office Upgrade Wizard.

To add this, select the ‘Exceptions’ tab, then ‘Add Program’.

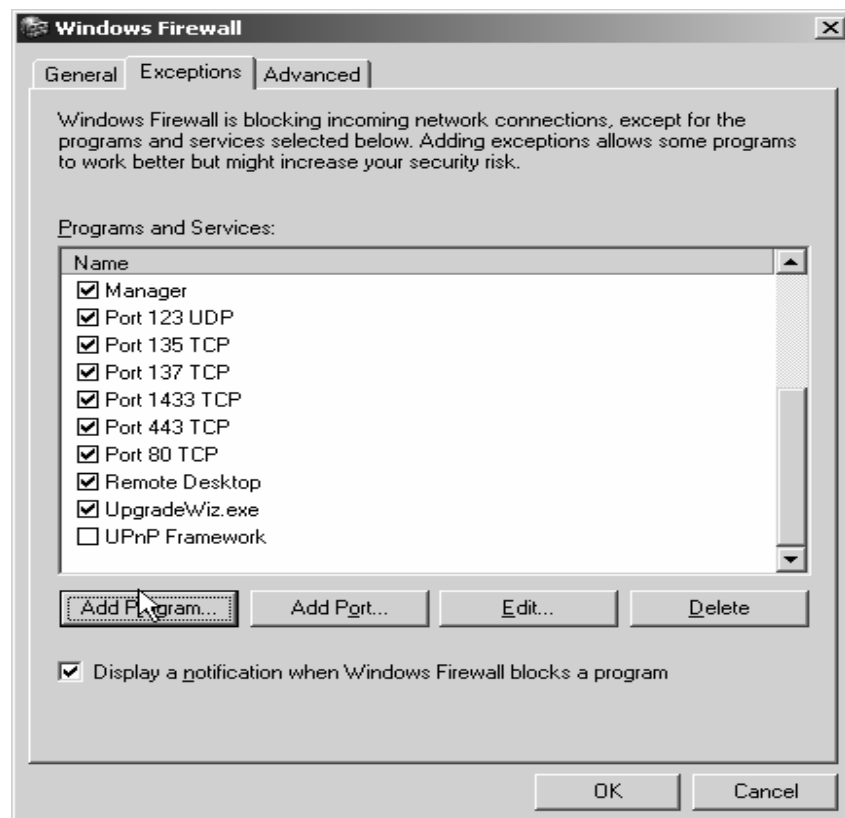
Browse to C:\Program Files\Avaya\IP Office\Manager\

Then select UpgradeWiz.exe

Select ‘OK’ to confirm the selection.



Select 'OK' to add the exception, then verify that the exception has been added by scrolling down to locate UpgradeWiz.exe.



Select 'OK' then 'OK' again to exit the network configuration applet.

Windows 2003 has now been set up allow IP Office Applications to work.

Call Status security changes

A Data Execution Prevention (DEP) exclusion needs to be entered for call status to work after Windows 2003 SP1 has been installed.

To do this, navigate to My computer, then select Properties, then Advanced, then Performance, settings, Data Execution Prevention.
Select the radio button for "Turn on DEP for all programs and services except those I select".



Select add, then browse to "callstatus.exe" which by default is found at:

"C:\Program Files\Avaya\IP Office\CallStatus\

Double click callstatus.exe and you will see it is added to the "exception list".

Leave it checked, then select OK, then OK again to confirm.

The Callstatus application should now work as expected.

Issued by:
Avaya SMBS Tier 4 Support
Contact details:-
EMEA/APAC
Tel: +44 1707 392200
Fax: +44 (0) 1707 376933
Email: gsstier4@avaya.com

NA/CALA
Tel: +1 732 852 1955
Fax: +1 732 852 1943
Email: IPOUST4ENG@Avaya.com

Internet: <http://www.avaya.com>
© 2005 Avaya Inc. All rights reserved.