# 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. Addition 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

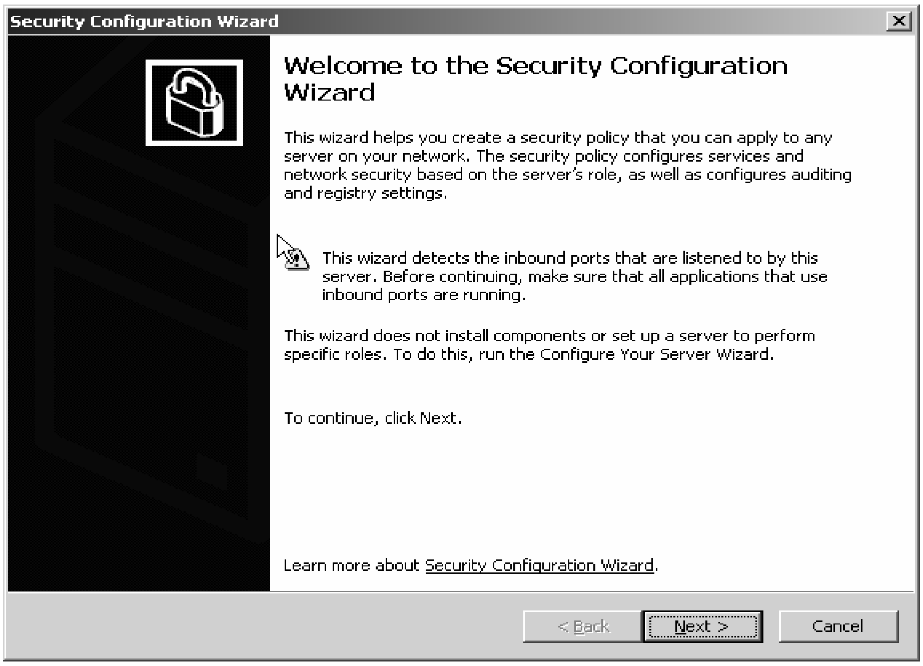
The security policy enforced by Service Pack 1 requires modifications in order for IP Office applications to work properly and maintain functionality. The following procedure documents the modifications needed for IP Office Voicemail Pro and IP Office Manager to function correctly.

### 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.



Security Configuration Wizard

Welcome to the Security Configuration Wizard

This wizard helps you create a security policy that you can apply to any server on your network. The security policy configures services and network security based on the server's role, as well as configures auditing and registry settings.

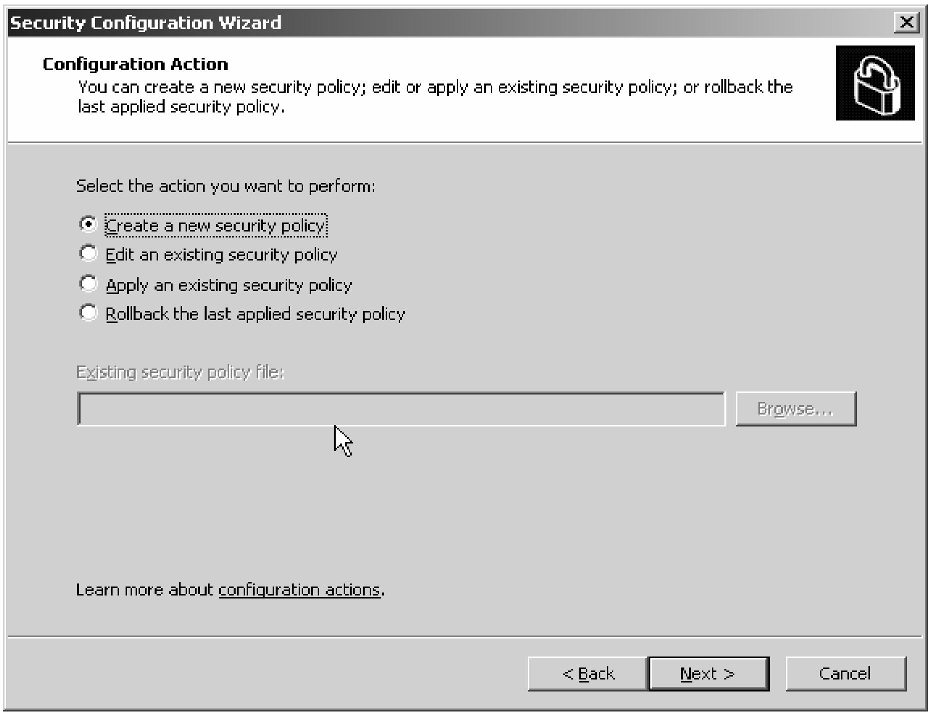
This wizard detects the inbound ports that are listened to by this server. Before continuing, make sure that all applications that use inbound ports are running.

This wizard does not install components or set up a server to perform specific roles. To do this, run the Configure Your Server Wizard.

To continue, click Next.

Learn more about Security Configuration Wizard.

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



Security Configuration Wizard

Configuration Action

You can create a new security policy; edit or apply an existing security policy; or rollback the last applied security policy.

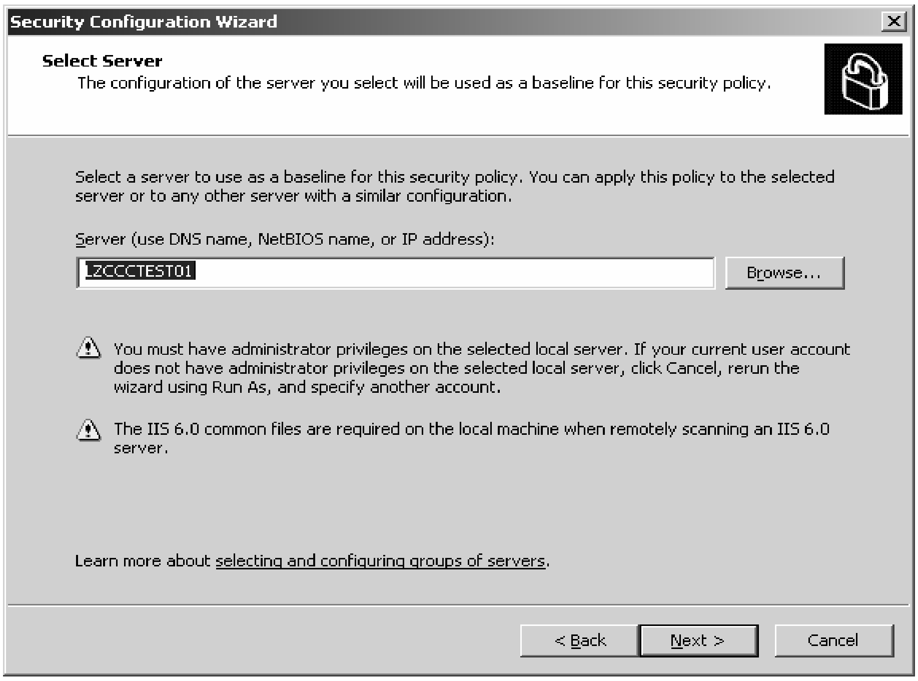
Select the action you want to perform:

● Create a new security policy
○ Edit an existing security policy
○ Apply an existing security policy
○ Rollback the last applied security policy

Existing security policy file:

Learn more about configuration actions.

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



Security Configuration Wizard

**Select Server**

The configuration of the server you select will be used as a baseline for this security policy.

Select a server to use as a baseline for this security policy. You can apply this policy to the selected server or to any other server with a similar configuration.

Server (use DNS name, NetBIOS name, or IP address):

LZCCCTEST01

Browse...

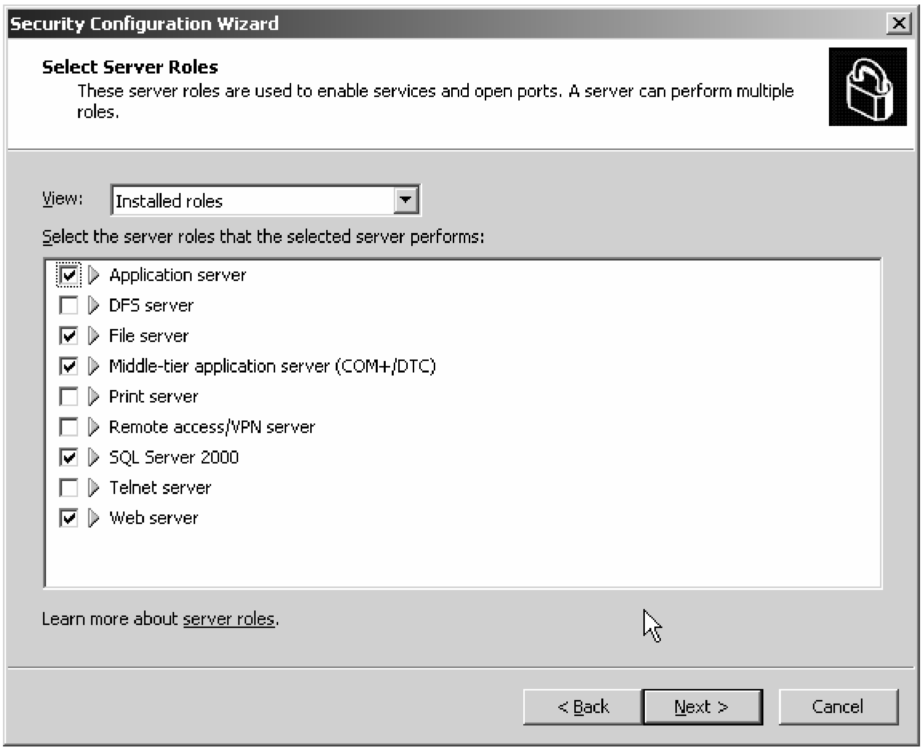
⚠ You must have administrator privileges on the selected local server. If your current user account does not have administrator privileges on the selected local server, click Cancel, rerun the wizard using Run As, and specify another account.

⚠ The IIS 6.0 common files are required on the local machine when remotely scanning an IIS 6.0 server.

Learn more about selecting and configuring groups of servers.

< Back | Next > | Cancel

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.



Security Configuration Wizard

**Select Server Roles**

These server roles are used to enable services and open ports. A server can perform multiple roles.

View: Installed roles

Select the server roles that the selected server performs:

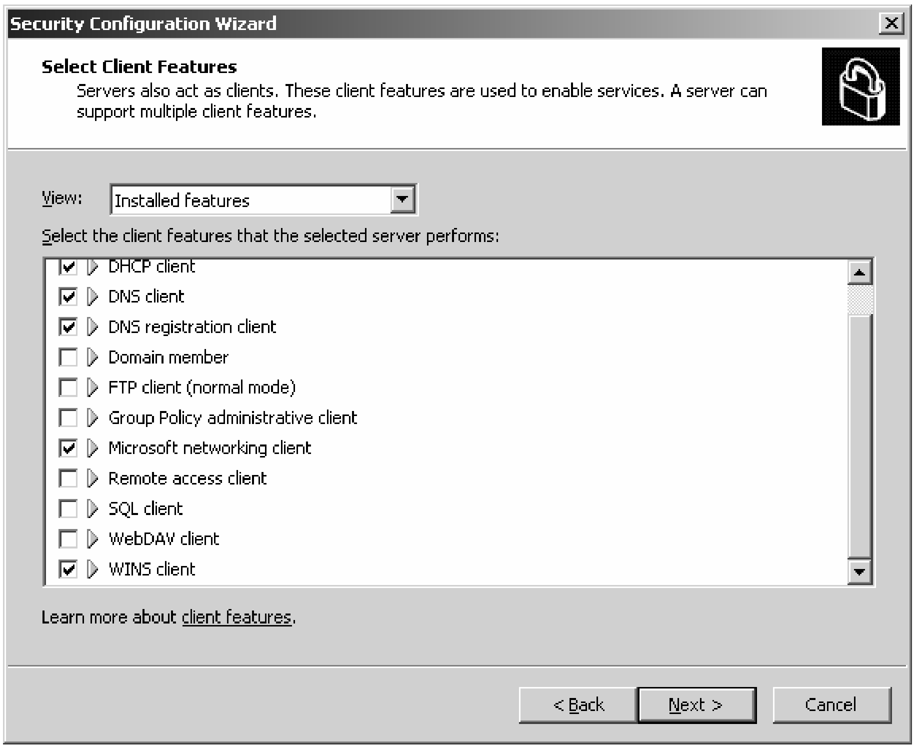
- ☑ Application server
- ☐ DFS server
- ☑ File server
- ☑ Middle-tier application server (COM+/DTC)
- ☐ Print server
- ☐ Remote access/VPN server
- ☑ SQL Server 2000
- ☐ Telnet server
- ☑ Web server

Learn more about server roles.

< Back | Next > | Cancel

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.



Security Configuration Wizard

**Select Client Features**

Servers also act as clients. These client features are used to enable services. A server can support multiple client features.

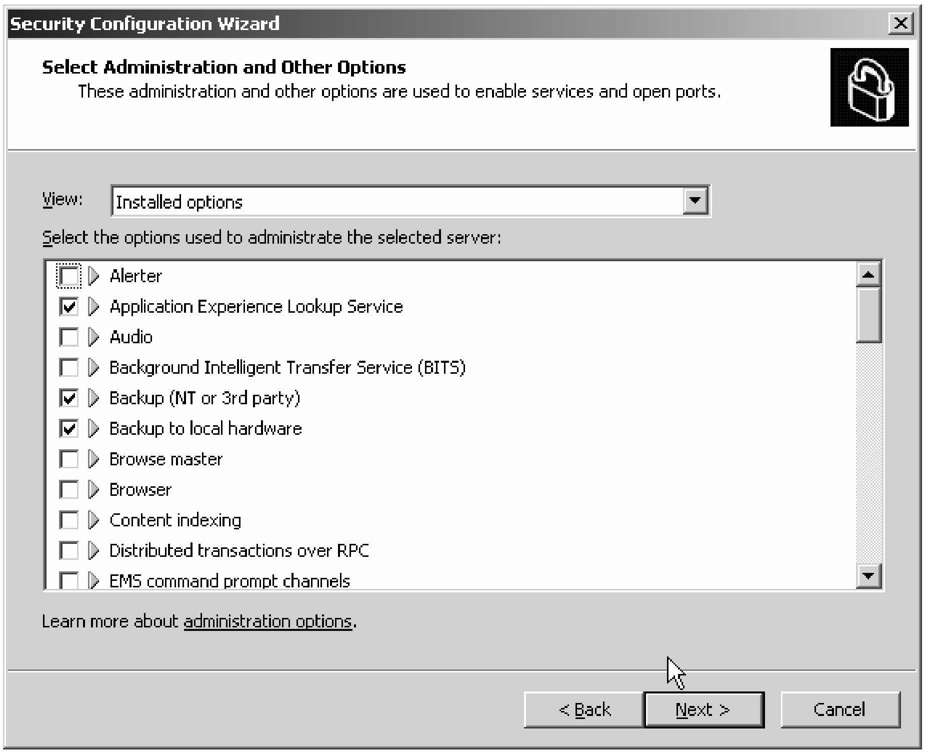
View: Installed features

Select the client features that the selected server performs:

- ☑ DHCP client
- ☑ DNS client
- ☑ DNS registration client
- □ Domain member
- □ FTP client (normal mode)
- □ Group Policy administrative client
- ☑ Microsoft networking client
- □ Remote access client
- □ SQL client
- □ WebDAV client
- ☑ WINS client

Learn more about client features.

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.



Security Configuration Wizard

**Select Administration and Other Options**

These administration and other options are used to enable services and open ports.

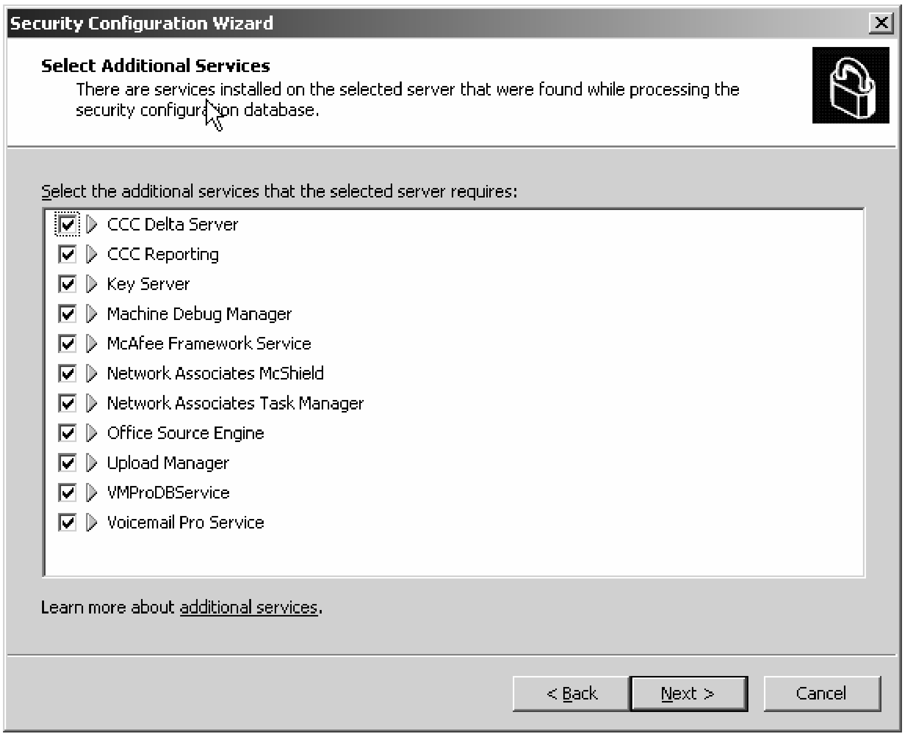
View: Installed options

Select the options used to administrate the selected server:

- □ Alerter
- ☑ Application Experience Lookup Service
- □ Audio
- □ Background Intelligent Transfer Service (BITS)
- ☑ Backup (NT or 3rd party)
- ☑ Backup to local hardware
- □ Browse master
- □ Browser
- □ Content indexing
- □ Distributed transactions over RPC
- □ EMS command prompt channels

Learn more about administration options.

The default ‘Installed options’ should be accepted by selecting ‘Next’.



Security Configuration Wizard

**Select Additional Services**

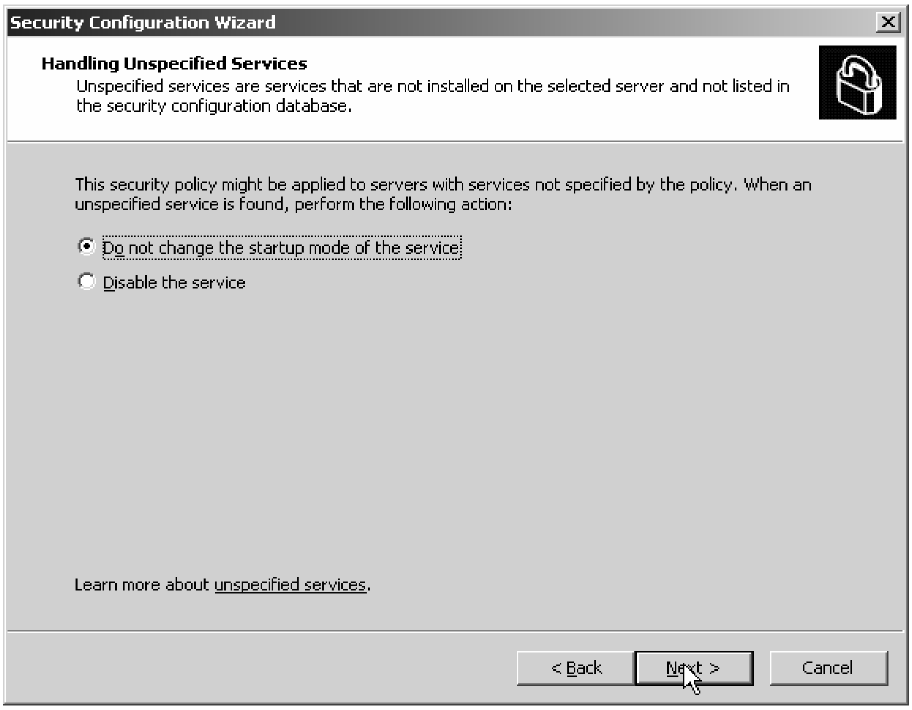
There are services installed on the selected server that were found while processing the security configuration database.

Select the additional services that the selected server requires:

- ☑ CCC Delta Server
- ☑ CCC Reporting
- ☑ Key Server
- ☑ Machine Debug Manager
- ☑ McAfee Framework Service
- ☑ Network Associates McShield
- ☑ Network Associates Task Manager
- ☑ Office Source Engine
- ☑ Upload Manager
- ☑ VMProDBService
- ☑ Voicemail Pro Service

Learn more about additional services.

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



Security Configuration Wizard

**Handling Unspecified Services**

Unspecified services are services that are not installed on the selected server and not listed in the security configuration database.

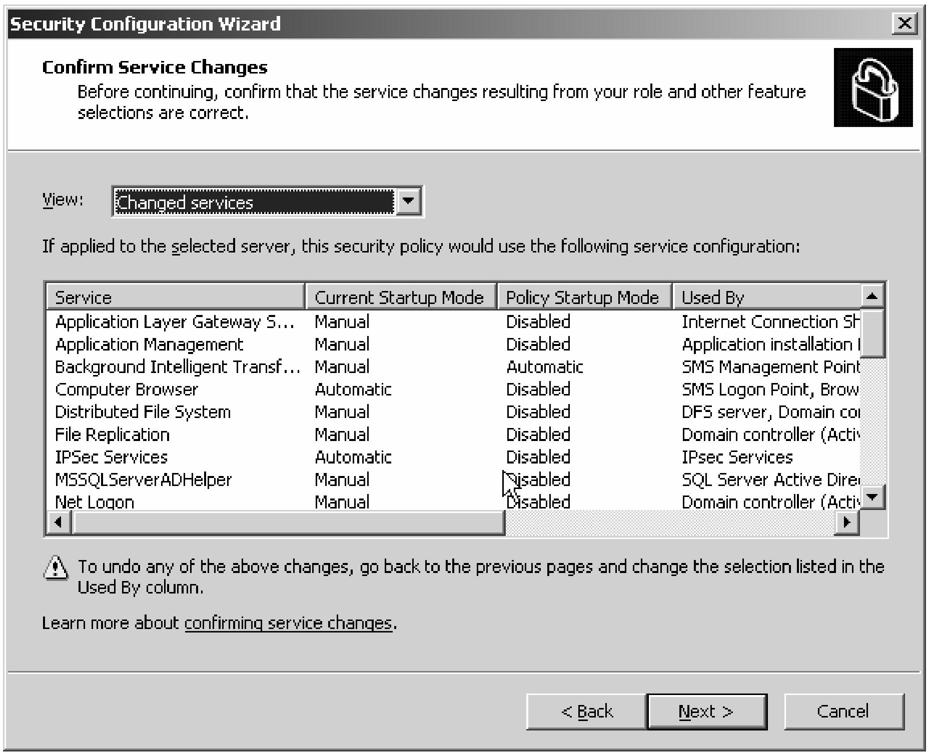
This security policy might be applied to servers with services not specified by the policy. When an unspecified service is found, perform the following action:

● Do not change the startup mode of the service

○ Disable the service

Learn more about unspecified services.

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

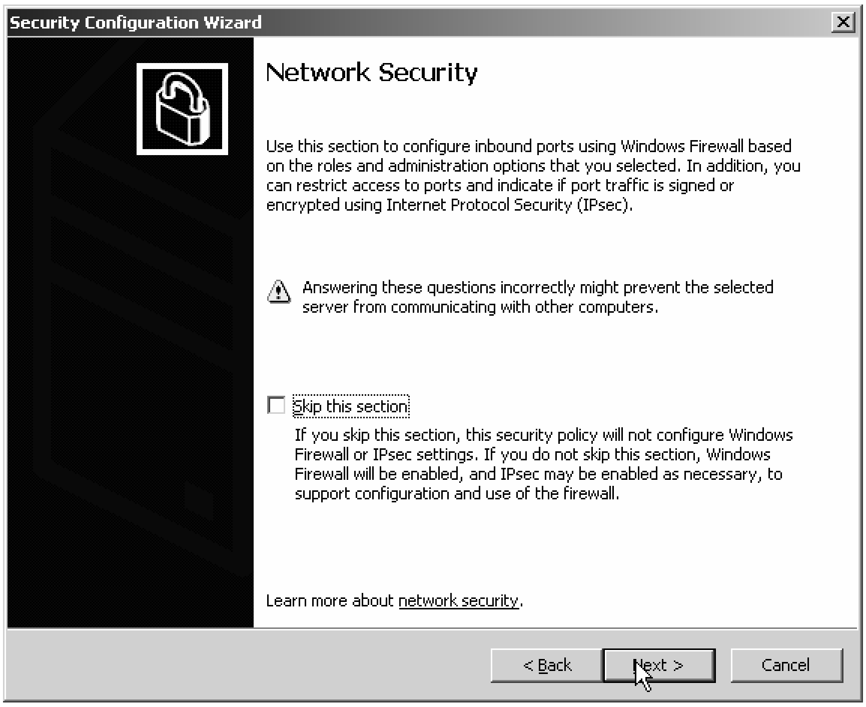
If applied to the selected server, this security policy would use the following service configuration:

| 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 co |
| File Replication | Manual | Disabled | Domain controller (Acti |
| IPSec Services | Automatic | Disabled | IPsec Services |
| MSSQLServerADHelper | Manual | Disabled | SQL Server Active Dire |
| Net Logon | Manual | Disabled | Domain controller (Acti |

⚠ 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.

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).

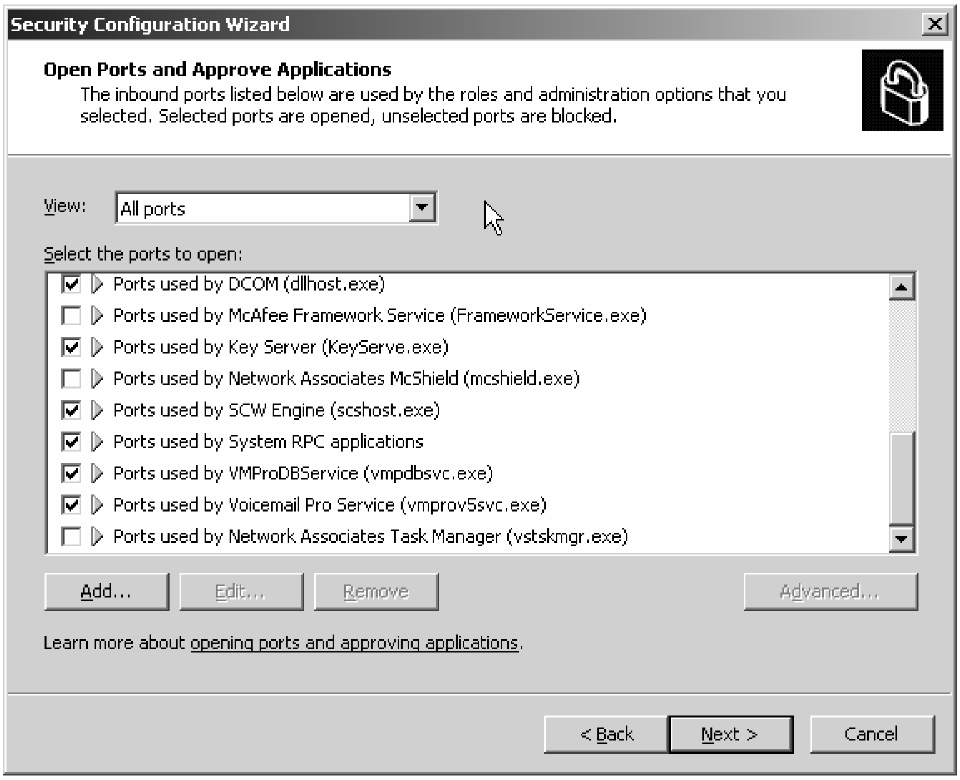
⚠ Answering these questions incorrectly might prevent the selected server from communicating with other computers.

□ 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.

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



Security Configuration Wizard

**Open Ports and Approve Applications**

The inbound ports listed below are used by the roles and administration options that you selected. Selected ports are opened, unselected ports are blocked.

View: All ports

Select the ports to open:

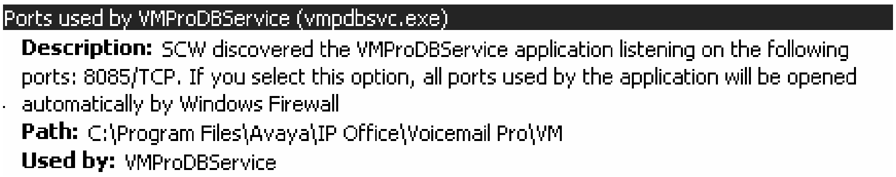
- ☑ Ports used by DCOM (dllhost.exe)
- ☐ Ports used by McAfee Framework Service (FrameworkService.exe)
- ☑ Ports used by Key Server (KeyServe.exe)
- ☐ Ports used by Network Associates McShield (mcshield.exe)
- ☑ Ports used by SCW Engine (scshost.exe)
- ☑ Ports used by System RPC applications
- ☑ Ports used by VMProDBService (vmpdbsvc.exe)
- ☑ Ports used by Voicemail Pro Service (vmprov5svc.exe)
- ☐ Ports used by Network Associates Task Manager (vstskmgr.exe)

Learn more about opening ports and approving applications.

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:-

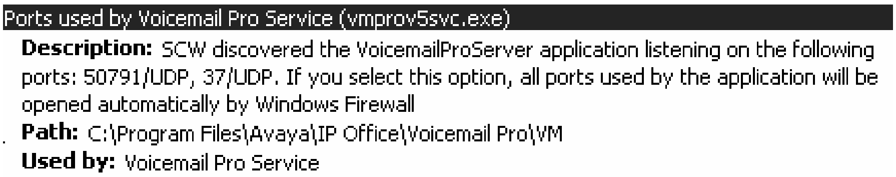
VoiceMail Pro Database Service –



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

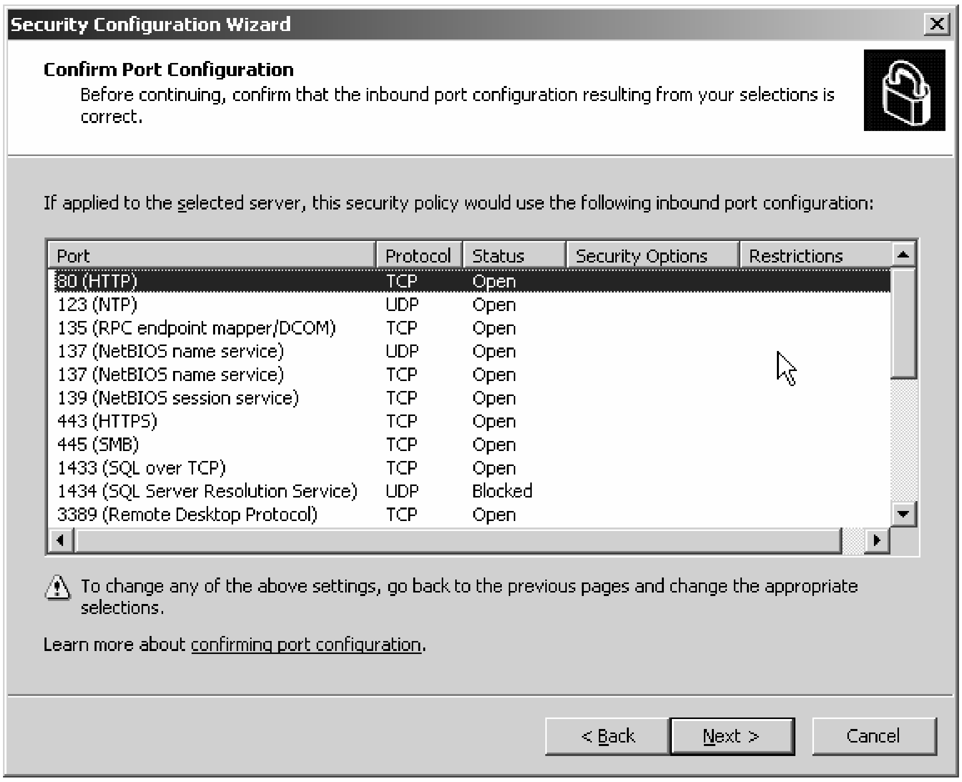
VoiceMail Pro Service –



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.



**Confirm Port Configuration**

Before continuing, confirm that the inbound port configuration resulting from your selections is correct.

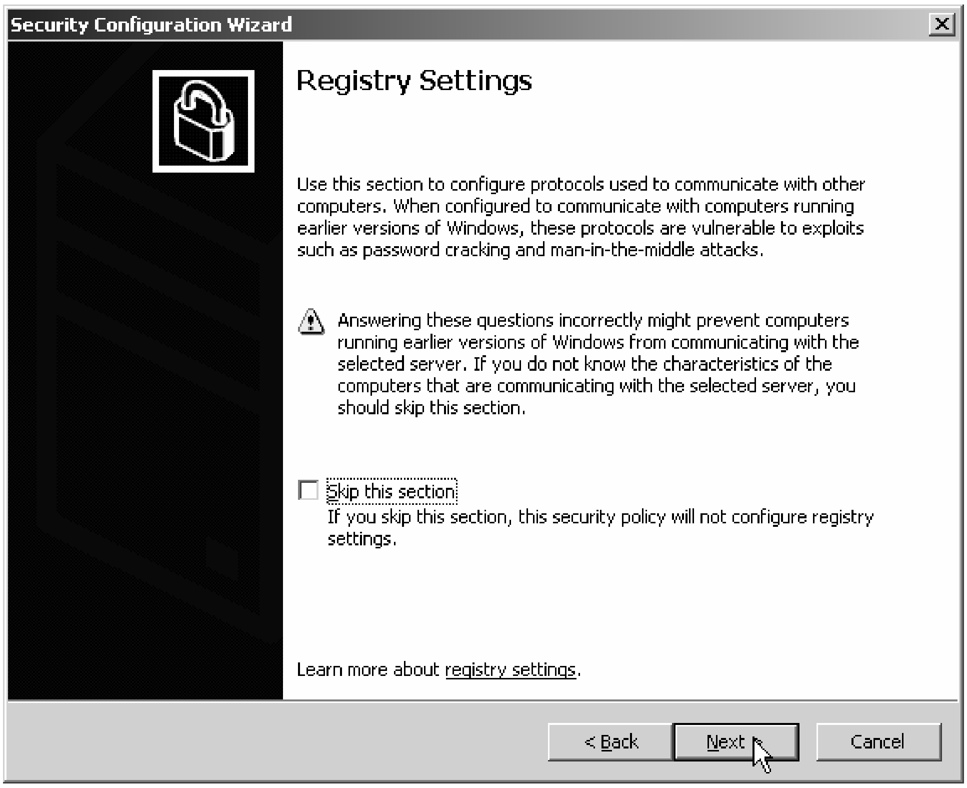
If applied to the selected server, this security policy would use the following inbound port configuration:

| Port | Protocol | Status | Security Options | Restrictions |
|---|---|---|---|---|
| 80 (HTTP) | TCP | Open | | |
| 123 (NTP) | UDP | Open | | |
| 135 (RPC endpoint mapper/DCOM) | TCP | Open | | |
| 137 (NetBIOS name service) | UDP | Open | | |
| 137 (NetBIOS name service) | TCP | Open | | |
| 139 (NetBIOS session service) | TCP | Open | | |
| 443 (HTTPS) | TCP | Open | | |
| 445 (SMB) | TCP | Open | | |
| 1433 (SQL over TCP) | TCP | Open | | |
| 1434 (SQL Server Resolution Service) | UDP | Blocked | | |
| 3389 (Remote Desktop Protocol) | TCP | Open | | |

To change any of the above settings, go back to the previous pages and change the appropriate selections.

Learn more about confirming port configuration.

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



## Registry Settings

Use this section to configure protocols used to communicate with other computers. When configured to communicate with computers running earlier versions of Windows, these protocols are vulnerable to exploits such as password cracking and man-in-the-middle attacks.

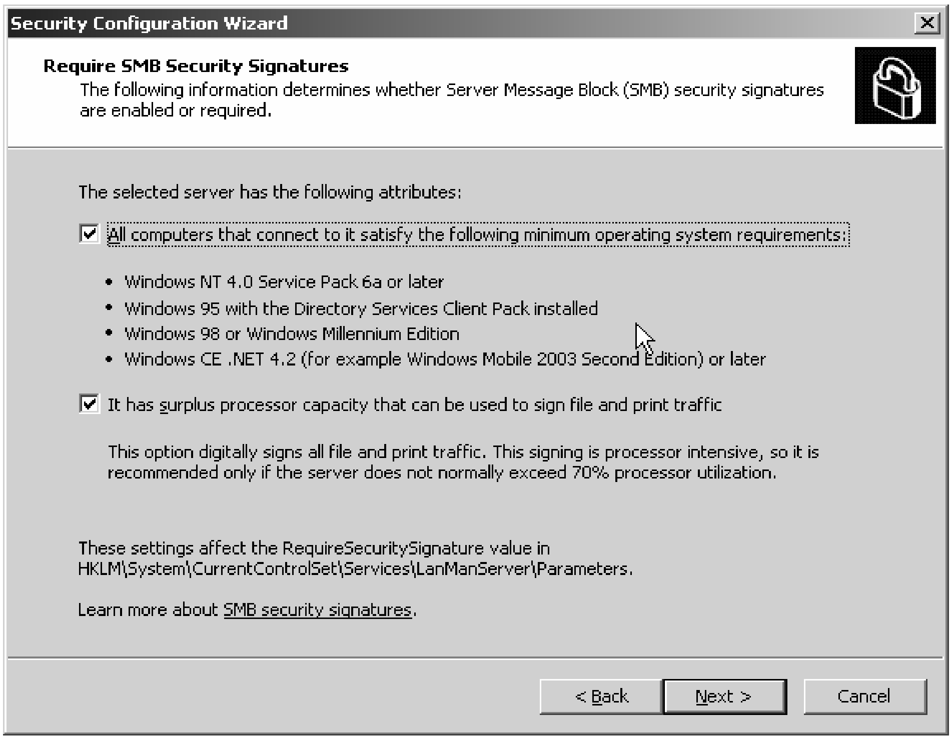
Answering these questions incorrectly might prevent computers running earlier versions of Windows from communicating with the selected server. If you do not know the characteristics of the computers that are communicating with the selected server, you should skip this section.

□ Skip this section

If you skip this section, this security policy will not configure registry settings.

Learn more about registry settings.

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



**Require SMB Security Signatures**

The following information determines whether Server Message Block (SMB) security signatures are enabled or required.

The selected server has the following attributes:

☑ All computers that connect to it satisfy the following minimum operating system requirements:

- Windows NT 4.0 Service Pack 6a or later
- Windows 95 with the Directory Services Client Pack installed
- Windows 98 or Windows Millennium Edition
- Windows CE .NET 4.2 (for example Windows Mobile 2003 Second Edition) or later

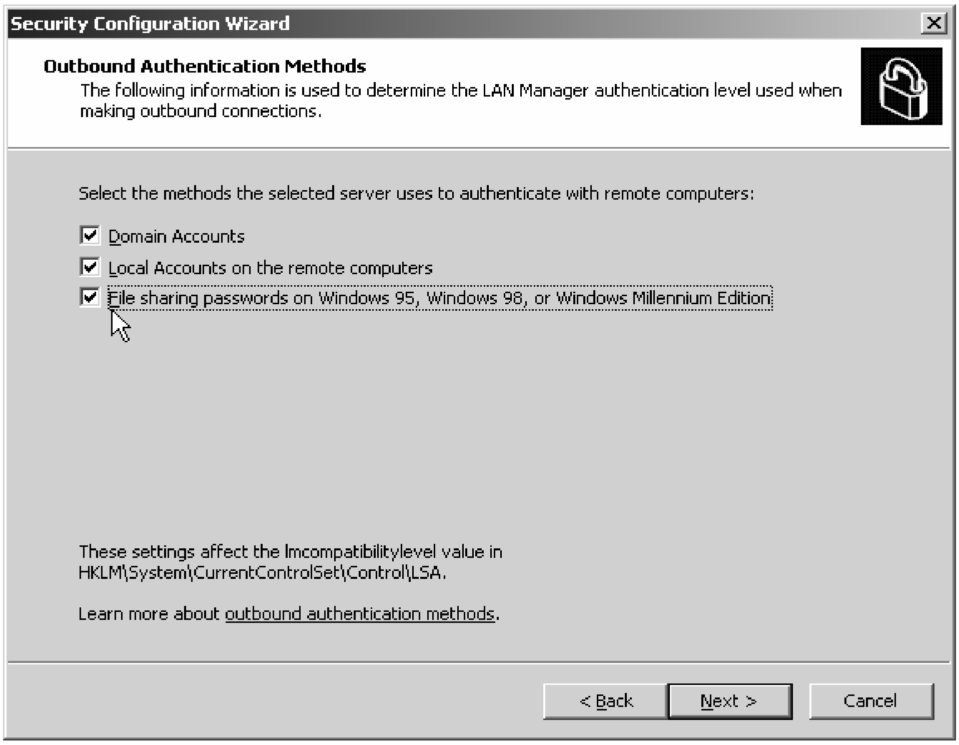
☑ It has surplus processor capacity that can be used to sign file and print traffic

This option digitally signs all file and print traffic. This signing is processor intensive, so it is recommended only if the server does not normally exceed 70% processor utilization.

These settings affect the RequireSecuritySignature value in HKLM\System\CurrentControlSet\Services\LanManServer\Parameters.

Learn more about SMB security signatures.

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



**Outbound Authentication Methods**

The following information is used to determine the LAN Manager authentication level used when making outbound connections.

Select the methods the selected server uses to authenticate with remote computers:

☑ Domain Accounts

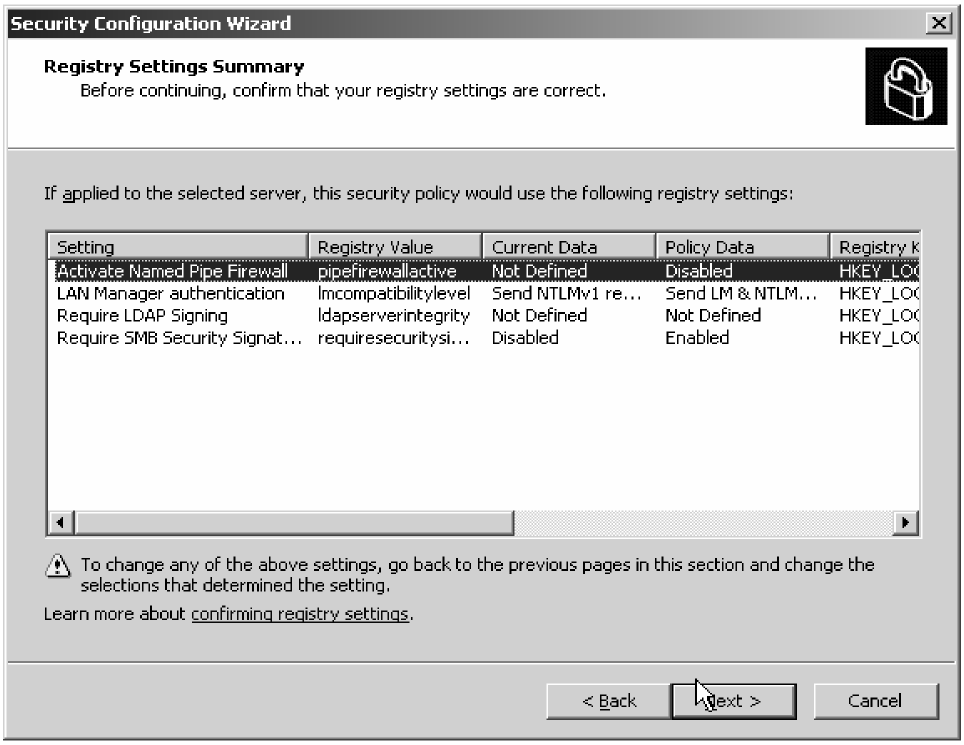
☑ Local Accounts on the remote computers

☑ File sharing passwords on Windows 95, Windows 98, or Windows Millennium Edition

These settings affect the lmcompatibilitylevel value in HKLM\System\CurrentControlSet\Control\LSA.

Learn more about outbound authentication methods.

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



**Registry Settings Summary**

Before continuing, confirm that your registry settings are correct.

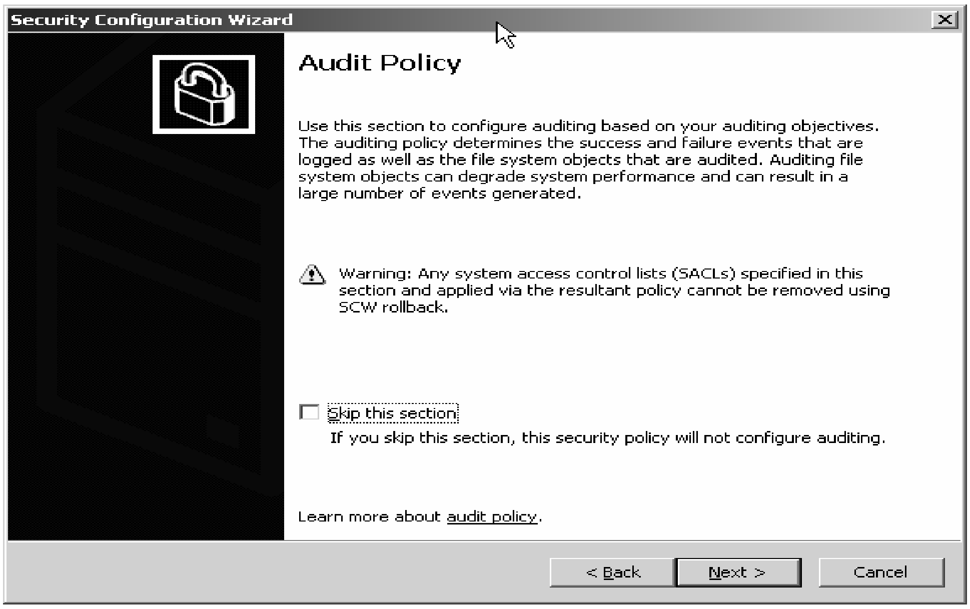
If applied to the selected server, this security policy would use the following registry settings:

| Setting | Registry Value | Current Data | Policy Data | Registry K |
|---|---|---|---|---|
| Activate Named Pipe Firewall | pipefirewallactive | Not Defined | Disabled | HKEY_LO( |
| LAN Manager authentication | lmcompatibilitylevel | Send NTLMv1 re... | Send LM & NTLM... | HKEY_LO( |
| Require LDAP Signing | ldapserverintegrity | Not Defined | Not Defined | HKEY_LO( |
| Require SMB Security Signat... | requiresecuritysi... | Disabled | Enabled | HKEY_LO( |

To change any of the above settings, go back to the previous pages in this section and change the selections that determined the setting.

Learn more about confirming registry settings.

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



Audit Policy

Use this section to configure auditing based on your auditing objectives. The auditing policy determines the success and failure events that are logged as well as the file system objects that are audited. Auditing file system objects can degrade system performance and can result in a large number of events generated.

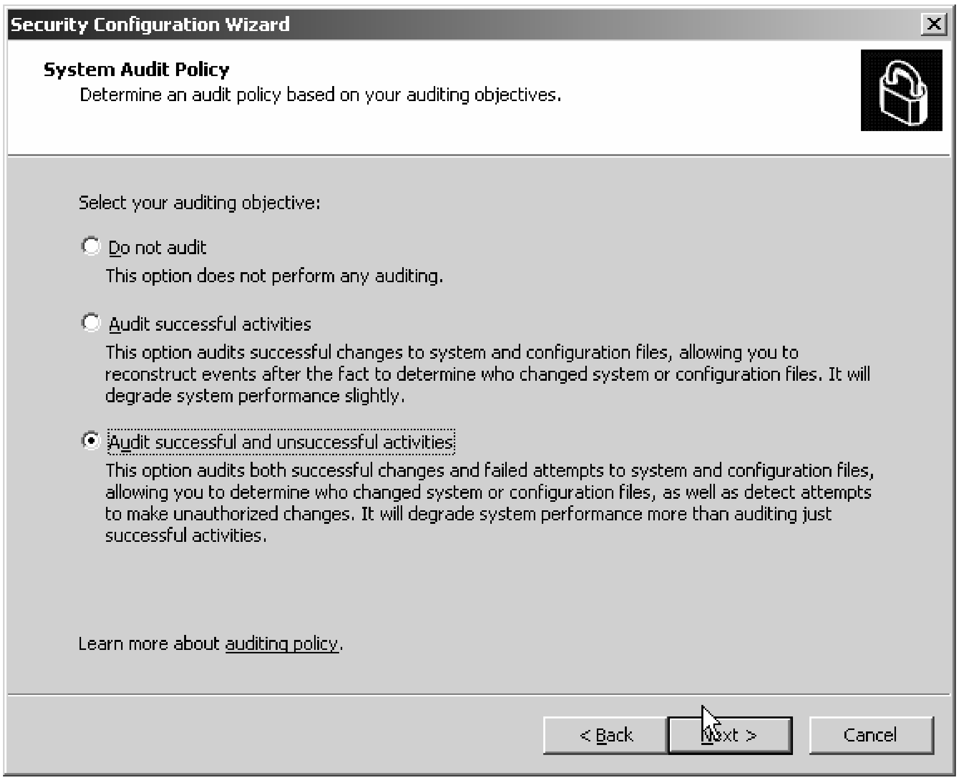
Warning: Any system access control lists (SACLs) specified in this section and applied via the resultant policy cannot be removed using SCW rollback.

□ Skip this section

If you skip this section, this security policy will not configure auditing.

Learn more about audit policy.

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



**System Audit Policy**
Determine an audit policy based on your auditing objectives.

Select your auditing objective:

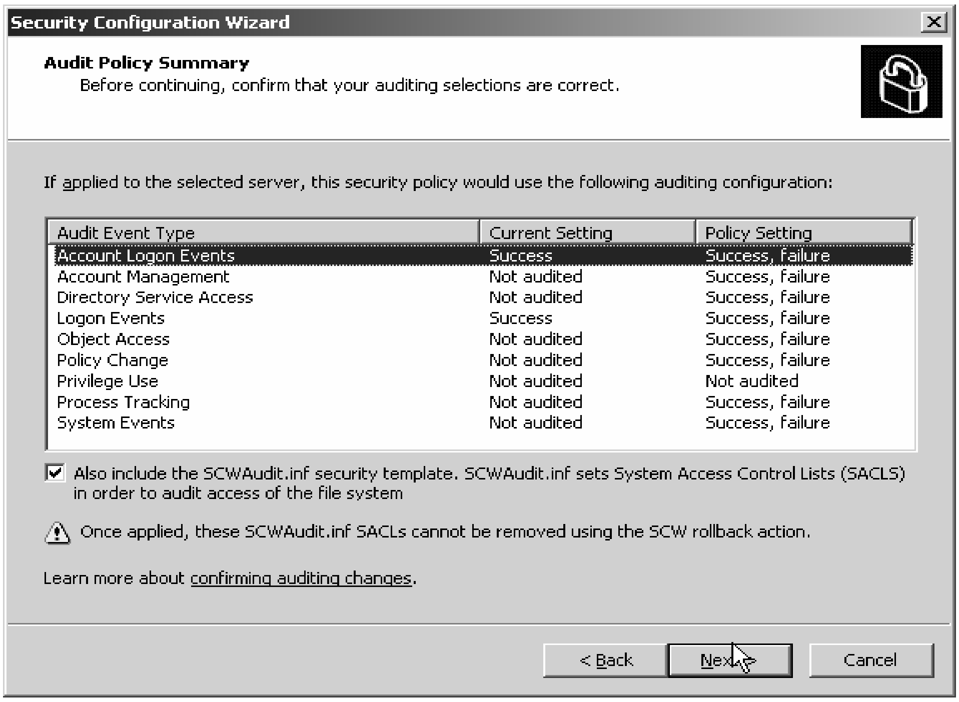
○ Do not audit
This option does not perform any auditing.

○ Audit successful activities
This option audits successful changes to system and configuration files, allowing you to reconstruct events after the fact to determine who changed system or configuration files. It will degrade system performance slightly.

● Audit successful and unsuccessful activities
This option audits both successful changes and failed attempts to system and configuration files, allowing you to determine who changed system or configuration files, as well as detect attempts to make unauthorized changes. It will degrade system performance more than auditing just successful activities.

Learn more about auditing policy.

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



**Audit Policy Summary**
Before continuing, confirm that your auditing selections are correct.

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

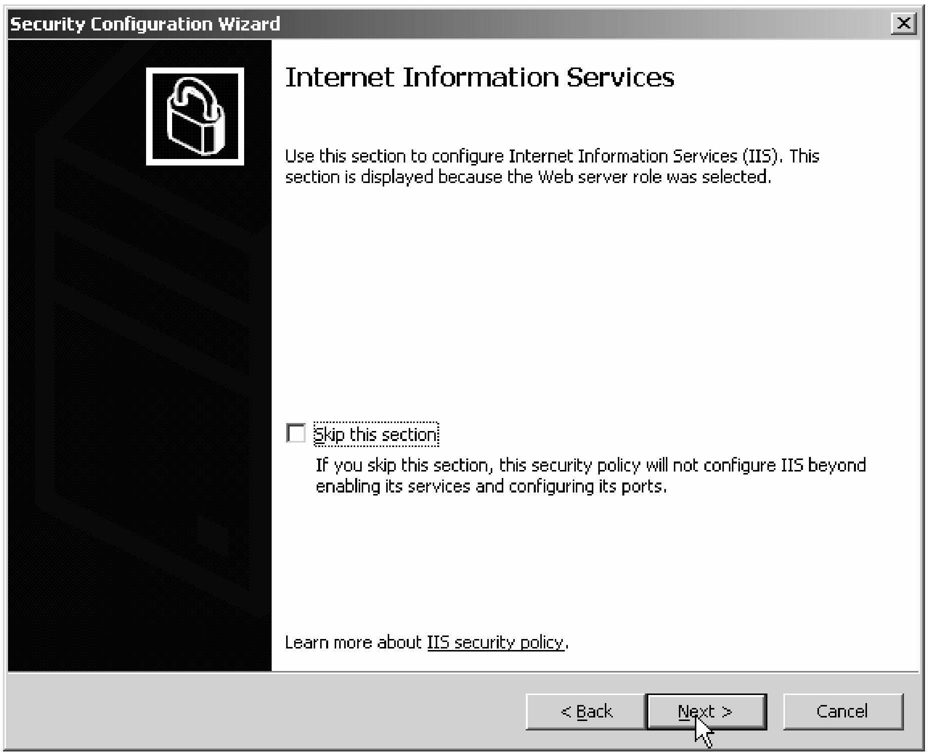
| Audit Event Type | Current Setting | Policy Setting |
|---|---|---|
| Account Logon Events | Success | Success, failure |
| Account Management | Not audited | Success, failure |
| Directory Service Access | Not audited | Success, failure |
| Logon Events | Success | Success, failure |
| Object Access | Not audited | Success, failure |
| Policy Change | Not audited | Success, failure |
| Privilege Use | Not audited | Not audited |
| Process Tracking | Not audited | Success, failure |
| System Events | Not audited | Success, failure |

☑ Also include the SCWAudit.inf security template. SCWAudit.inf sets System Access Control Lists (SACLS) in order to audit access of the file system

⚠ Once applied, these SCWAudit.inf SACLs cannot be removed using the SCW rollback action.

Learn more about confirming auditing changes.

Review and confirm the selected audit policy by selecting ‘Next’.



Security Configuration Wizard

Internet Information Services

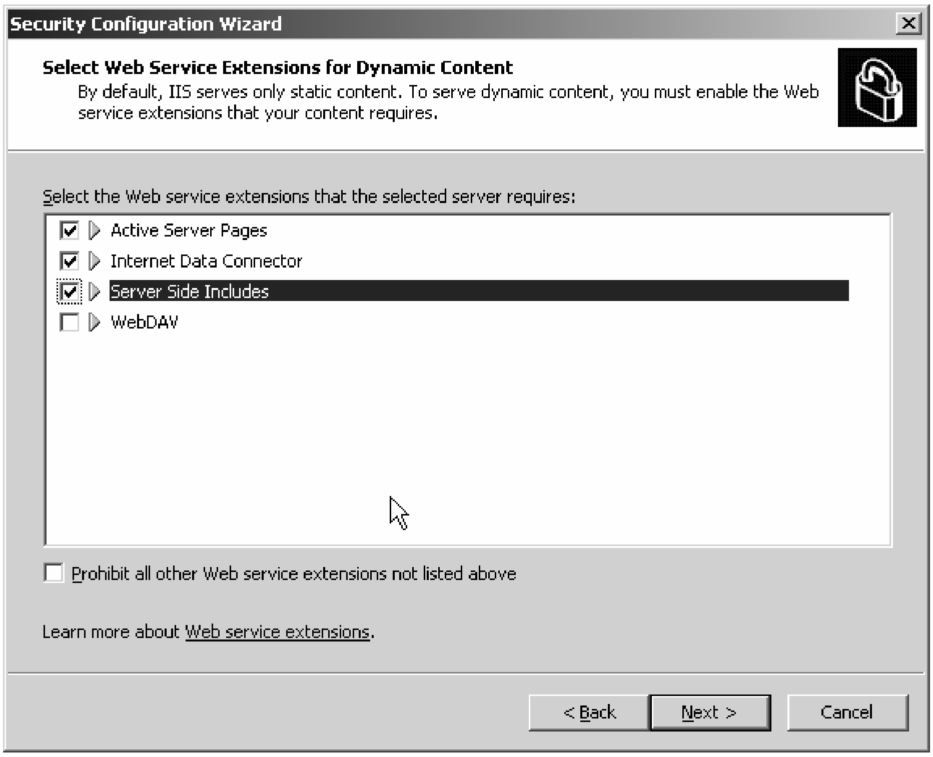
Use this section to configure Internet Information Services (IIS). This section is displayed because the Web server role was selected.

□ Skip this section

If you skip this section, this security policy will not configure IIS beyond enabling its services and configuring its ports.

Learn more about IIS security policy.

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



Security Configuration Wizard

**Select Web Service Extensions for Dynamic Content**

By default, IIS serves only static content. To serve dynamic content, you must enable the Web service extensions that your content requires.

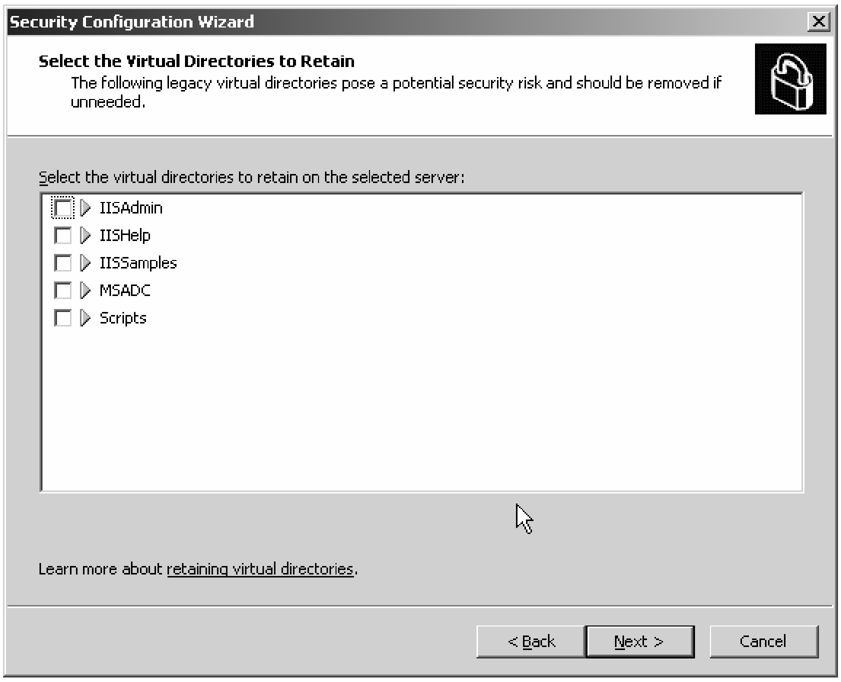
Select the Web service extensions that the selected server requires:

- ☑ Active Server Pages
- ☑ Internet Data Connector
- ☑ Server Side Includes
- □ WebDAV

□ Prohibit all other Web service extensions not listed above

Learn more about Web service extensions.

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



Security Configuration Wizard

**Select the Virtual Directories to Retain**

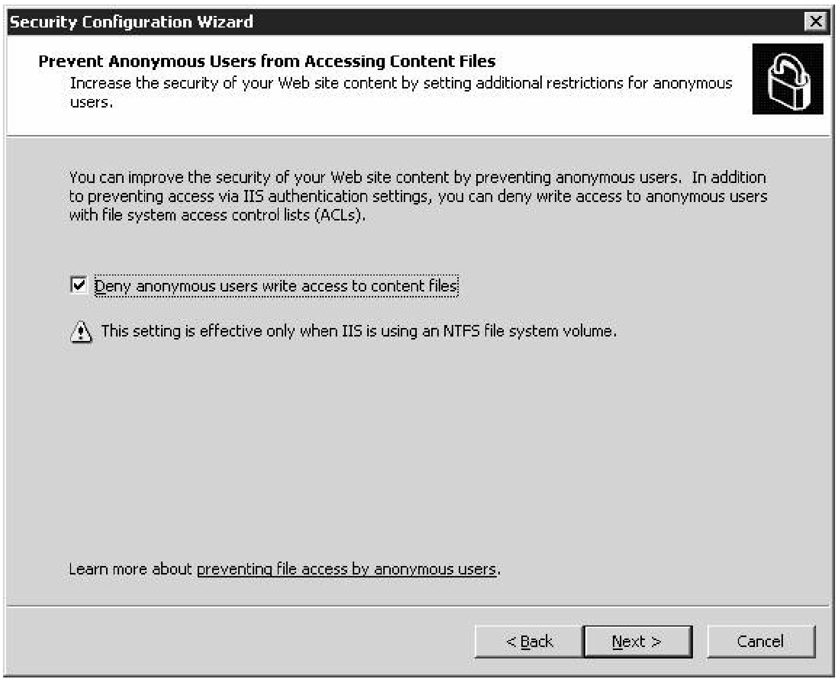
The following legacy virtual directories pose a potential security risk and should be removed if unneeded.

Select the virtual directories to retain on the selected server:

- □ IISAdmin
- □ IISHelp
- □ IISSamples
- □ MSADC
- □ Scripts

Learn more about retaining virtual directories.

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.



Security Configuration Wizard

**Prevent Anonymous Users from Accessing Content Files**

Increase the security of your Web site content by setting additional restrictions for anonymous users.

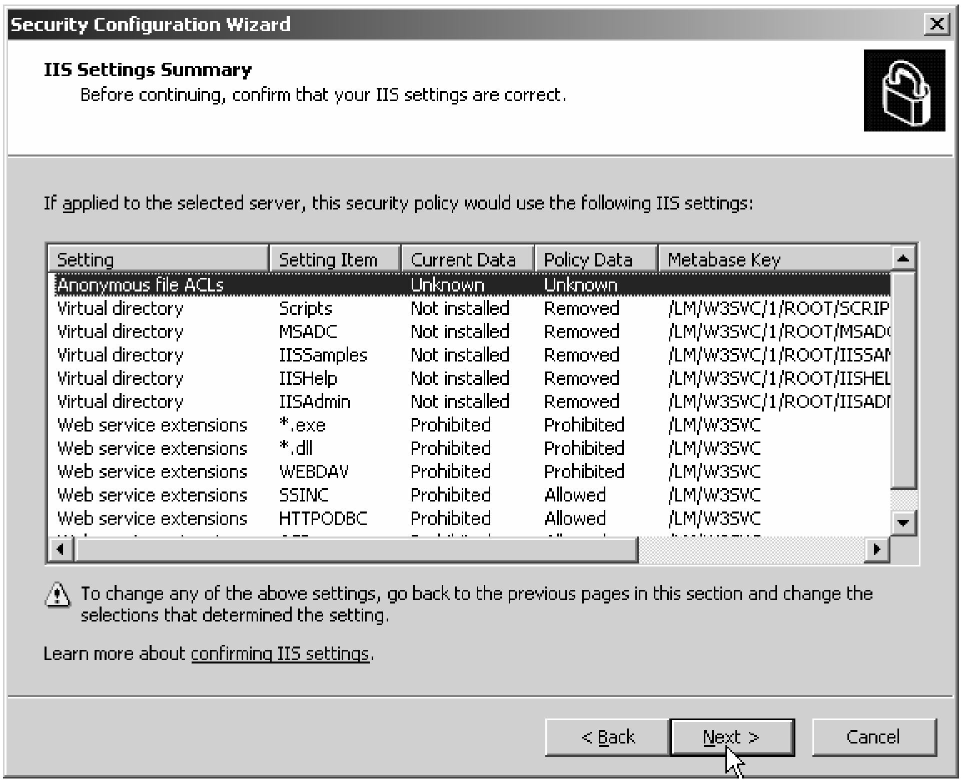
You can improve the security of your Web site content by preventing anonymous users. In addition to preventing access via IIS authentication settings, you can deny write access to anonymous users with file system access control lists (ACLs).

☑ Deny anonymous users write access to content files

⚠ This setting is effective only when IIS is using an NTFS file system volume.

Learn more about preventing file access by anonymous users.

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.



Security Configuration Wizard

**IIS Settings Summary**
Before continuing, confirm that your IIS settings are correct.

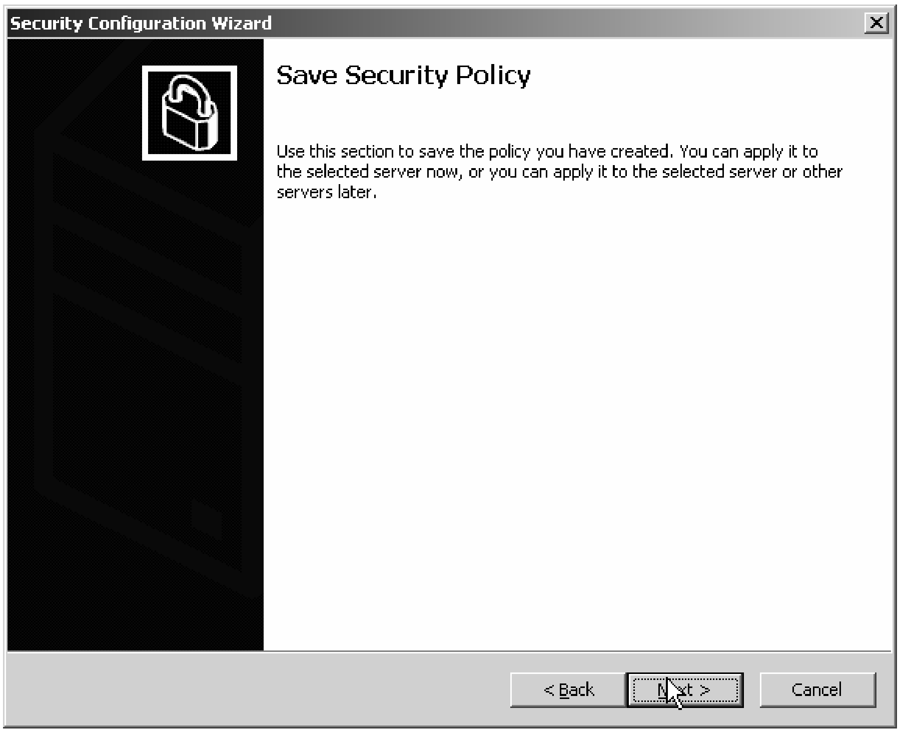
If applied to the selected server, this security policy would use the following IIS settings:

| Setting | Setting Item | Current Data | Policy Data | Metabase Key |
|---|---|---|---|---|
| Anonymous file ACLs | | Unknown | Unknown | |
| Virtual directory | Scripts | Not installed | Removed | /LM/W3SVC/1/ROOT/SCRIP |
| Virtual directory | MSADC | Not installed | Removed | /LM/W3SVC/1/ROOT/MSAD( |
| Virtual directory | IISSamples | Not installed | Removed | /LM/W3SVC/1/ROOT/IISSAI |
| Virtual directory | IISHelp | Not installed | Removed | /LM/W3SVC/1/ROOT/IISHEL |
| Virtual directory | IISAdmin | Not installed | Removed | /LM/W3SVC/1/ROOT/IISADI |
| Web service extensions | *.exe | Prohibited | Prohibited | /LM/W3SVC |
| Web service extensions | *.dll | Prohibited | Prohibited | /LM/W3SVC |
| Web service extensions | WEBDAV | Prohibited | Prohibited | /LM/W3SVC |
| Web service extensions | SSINC | Prohibited | Allowed | /LM/W3SVC |
| Web service extensions | HTTPODBC | Prohibited | Allowed | /LM/W3SVC |

To change any of the above settings, go back to the previous pages in this section and change the selections that determined the setting.

Learn more about confirming IIS settings.

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

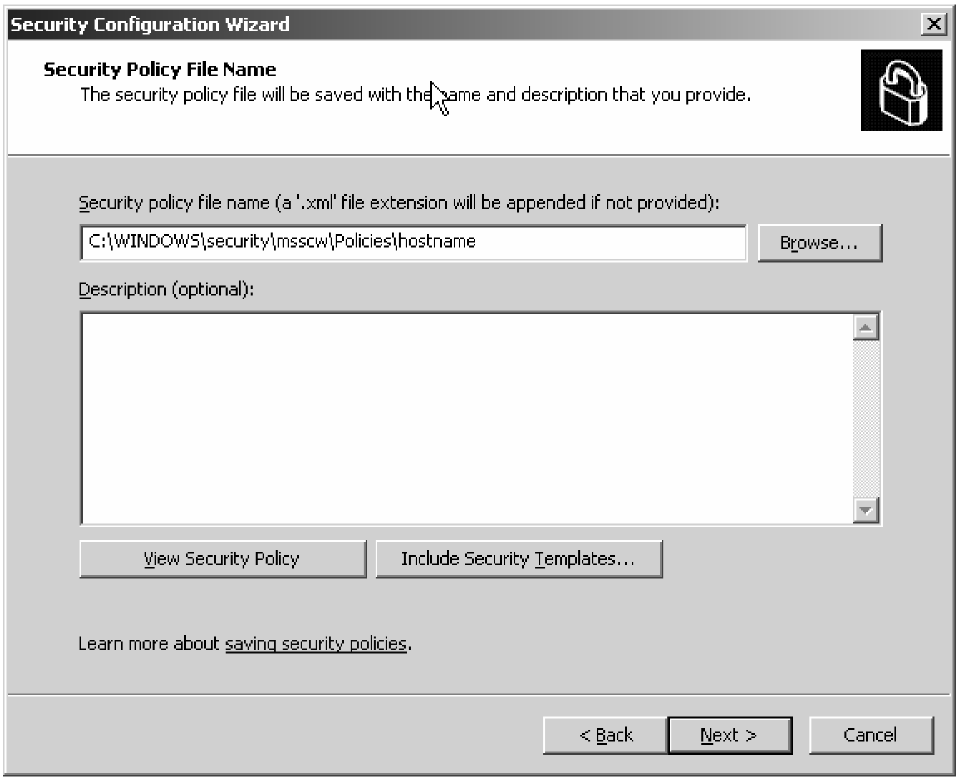


Security Configuration Wizard

Save Security Policy

Use this section to save the policy you have created. You can apply it to the selected server now, or you can apply it to the selected server or other servers later.

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



Security Configuration Wizard

**Security Policy File Name**

The security policy file will be saved with the name and description that you provide.

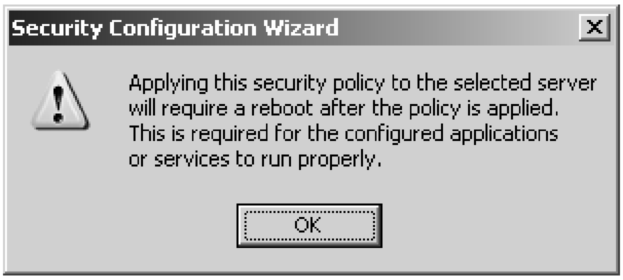
Security policy file name (a '.xml' file extension will be appended if not provided):

C:\WINDOWS\security\msscw\Policies\hostname

Description (optional):

Browse...
View Security Policy
Include Security Templates...
Learn more about saving security policies.
< Back
Next >
Cancel

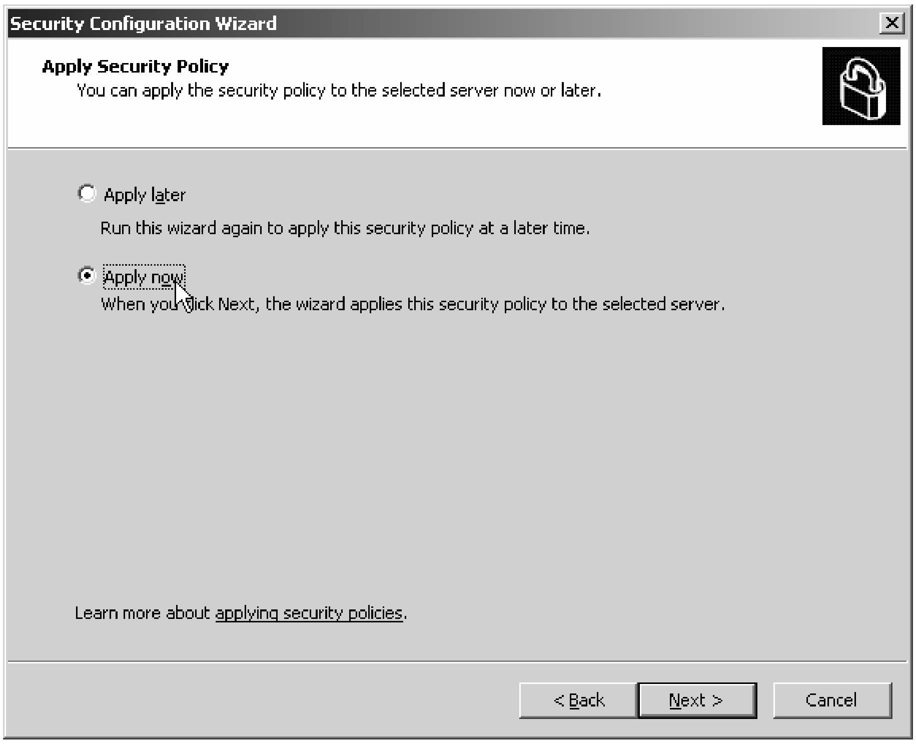
Enter a filename (the PCs hostname) to replace ‘hostname’, then select ‘Next’ to continue.



Security Configuration Wizard

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.

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



Security Configuration Wizard

**Apply Security Policy**

You can apply the security policy to the selected server now or later.

○ Apply later

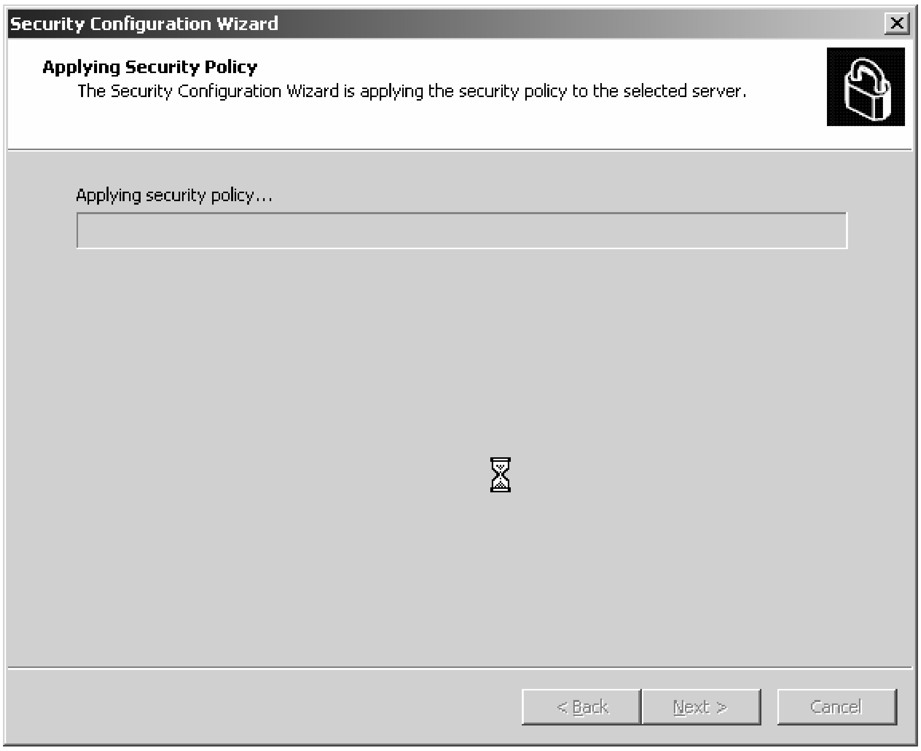
Run this wizard again to apply this security policy at a later time.

● Apply now

When you click Next, the wizard applies this security policy to the selected server.

Learn more about applying security policies.

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



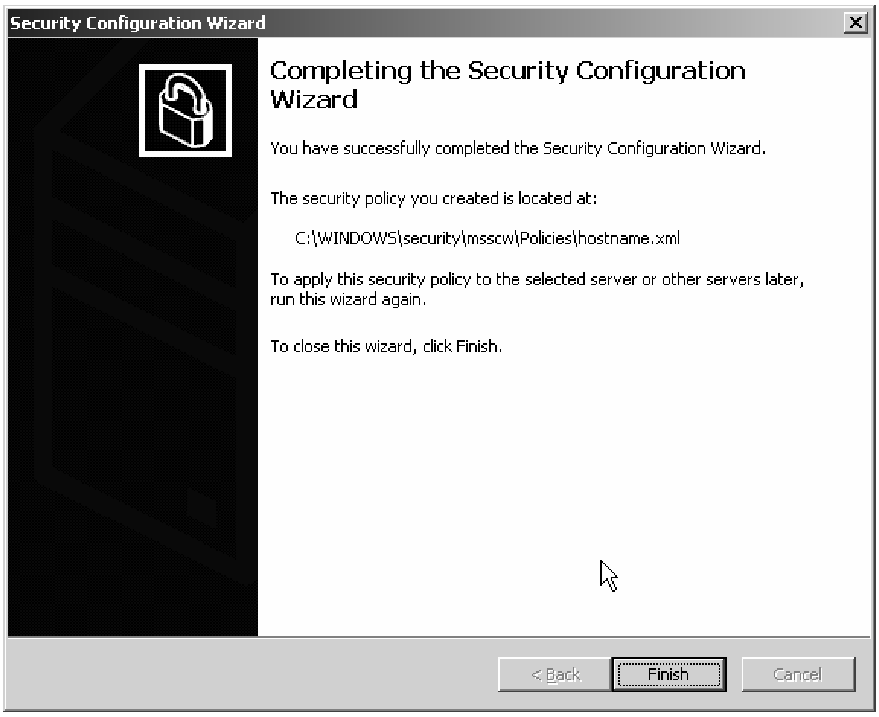
Security Configuration Wizard

**Applying Security Policy**

The Security Configuration Wizard is applying the security policy to the selected server.

Applying security policy...

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



Completing the Security Configuration Wizard

You have successfully completed the Security Configuration Wizard.

The security policy you created is located at:

C:\WINDOWS\security\msscw\Policies\hostname.xml

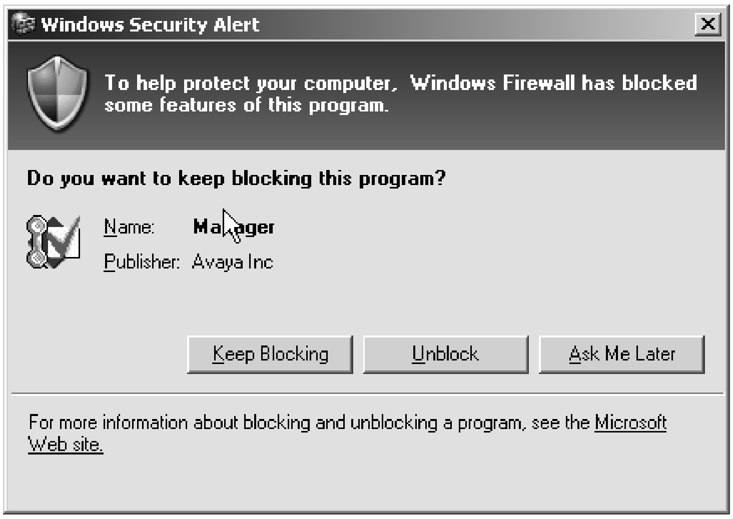
To apply this security policy to the selected server or other servers later, run this wizard again.

To close this wizard, click Finish.

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:



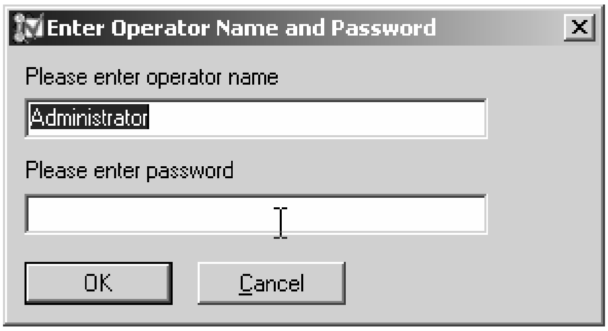
To help protect your computer, Windows Firewall has blocked some features of this program.

Do you want to keep blocking this program?

Name: Manager
Publisher: Avaya Inc

For more information about blocking and unblocking a program, see the Microsoft Web site.

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



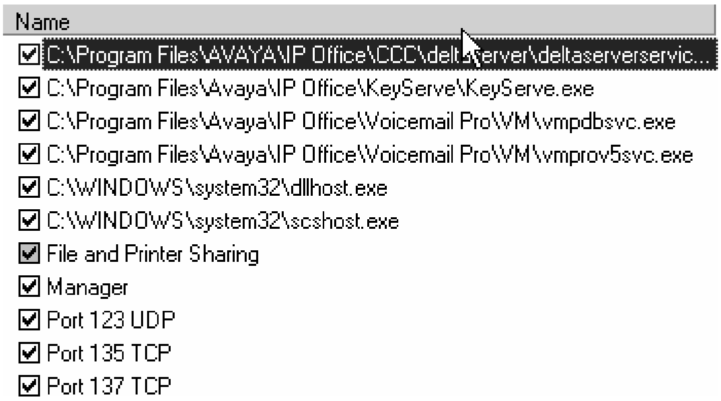
Please enter operator name

Administrator

Please enter password

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:



Name

- ☑ C:\Program Files\AVAYA\IP Office\CCC\deltaserver\deltaserverservic...
- ☑ C:\Program Files\Avaya\IP Office\KeyServe\KeyServe.exe
- ☑ C:\Program Files\Avaya\IP Office\Voicemail Pro\VM\vmpdbsvc.exe
- ☑ C:\Program Files\Avaya\IP Office\Voicemail Pro\VM\vmprov5svc.exe
- ☑ C:\WINDOWS\system32\dllhost.exe
- ☑ C:\WINDOWS\system32\scshost.exe
- ☑ File and Printer Sharing
- ☑ Manager
- ☑ Port 123 UDP
- ☑ Port 135 TCP
- ☑ Port 137 TCP

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

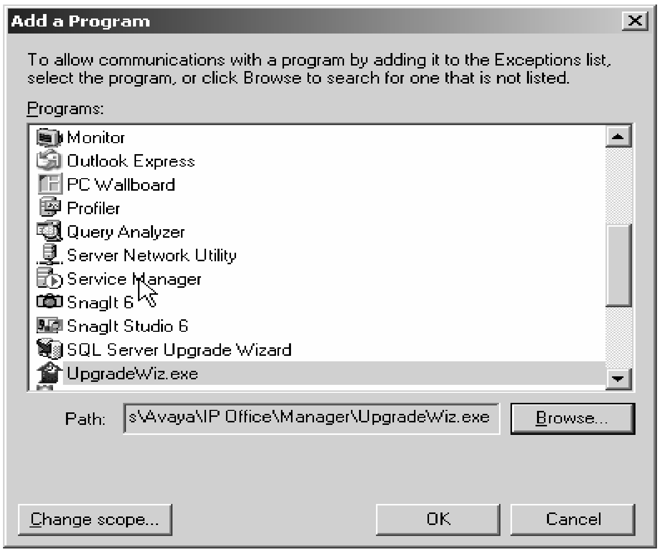
An exception is also required for the IP Office Upgrade Wizard.

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.



Add a Program

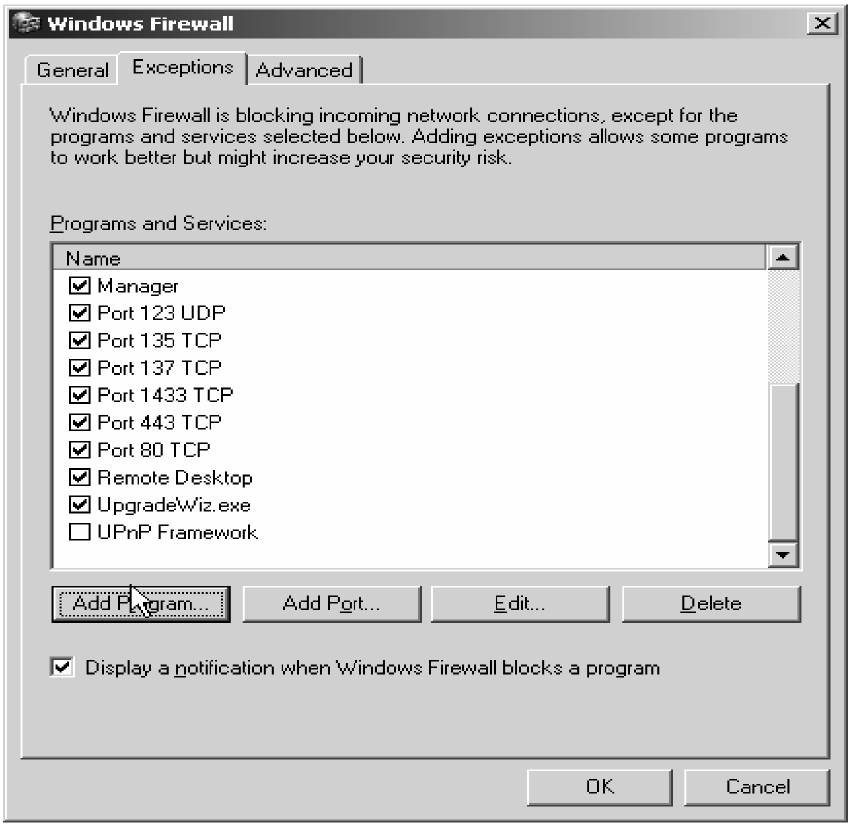
To allow communications with a program by adding it to the Exceptions list, select the program, or click Browse to search for one that is not listed.

Programs:

- Monitor
- Outlook Express
- PC Wallboard
- Profiler
- Query Analyzer
- Server Network Utility
- Service Manager
- SnagIt 6
- SnagIt Studio 6
- SQL Server Upgrade Wizard
- UpgradeWiz.exe

Path: s\Avaya\IP Office\Manager\UpgradeWiz.exe

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



Windows Firewall

Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.

Programs and Services:

Name

- ☑ Manager
- ☑ Port 123 UDP
- ☑ Port 135 TCP
- ☑ Port 137 TCP
- ☑ Port 1433 TCP
- ☑ Port 443 TCP
- ☑ Port 80 TCP
- ☑ Remote Desktop
- ☑ UpgradeWiz.exe
- □ UPnP Framework

☑ Display a notification when Windows Firewall blocks a program

Select ‘OK’ then ‘OK’ again to exit the network configuration applet.

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

*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*