

Microsoft SCW (Security Configuration Wizard)

About the SCW

SCW disables unnecessary services and provides Windows Firewall with Advanced Security support

Removes unused firewall rules based on Server Roles

SCW enables those services that are necessary for the server, based on the roles that you select on the Select Server Roles page

The following procedure will lock down the Server 2008 system completely, I'm calling this tool the secret weapon for this contest. It's going to disable un-necessary services, & lock down the whole environment.

To launch the SCW type scw at an Administrator Command Prompt



Select Next. Create a new security policy, Next

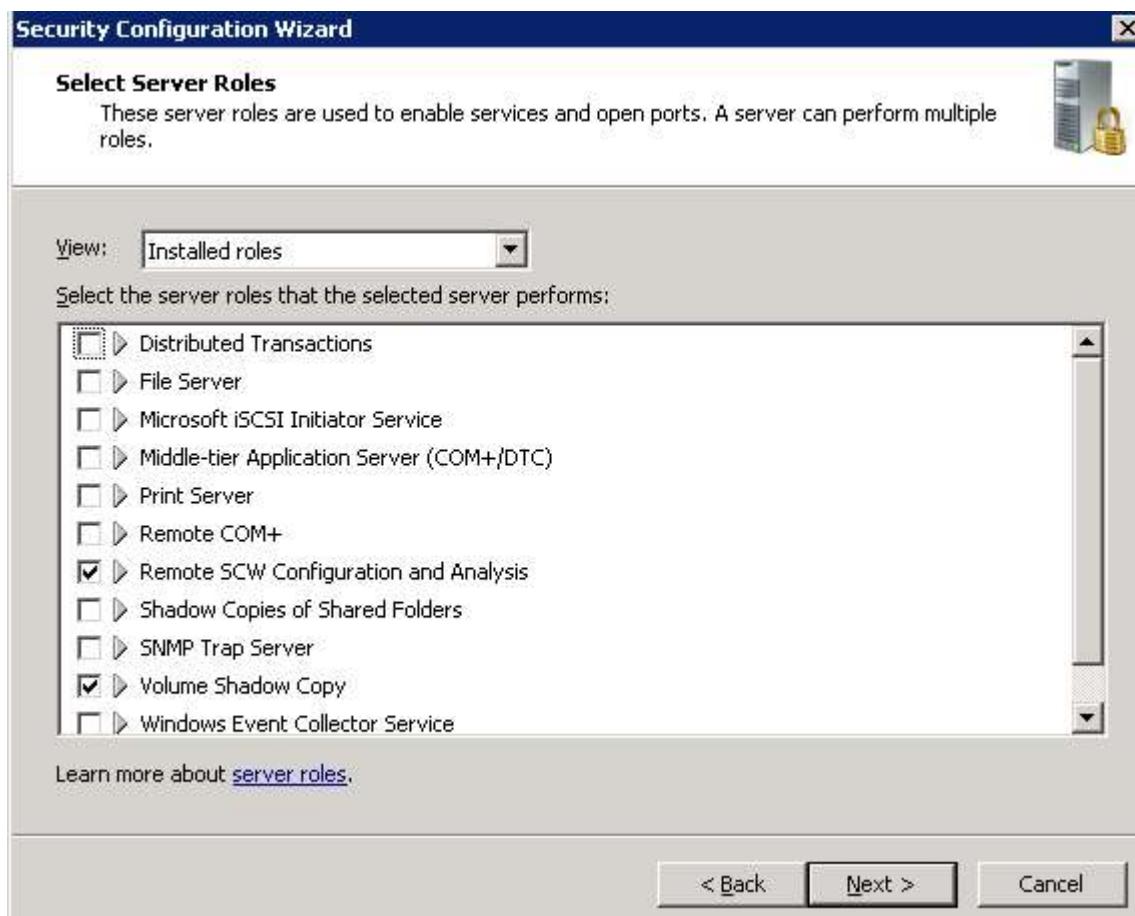


Enter hostname or LOCALHOST (to identify the computers' hostname, you can type hostname at an Administrator Command Prompt), Next

Processing Complete, Next

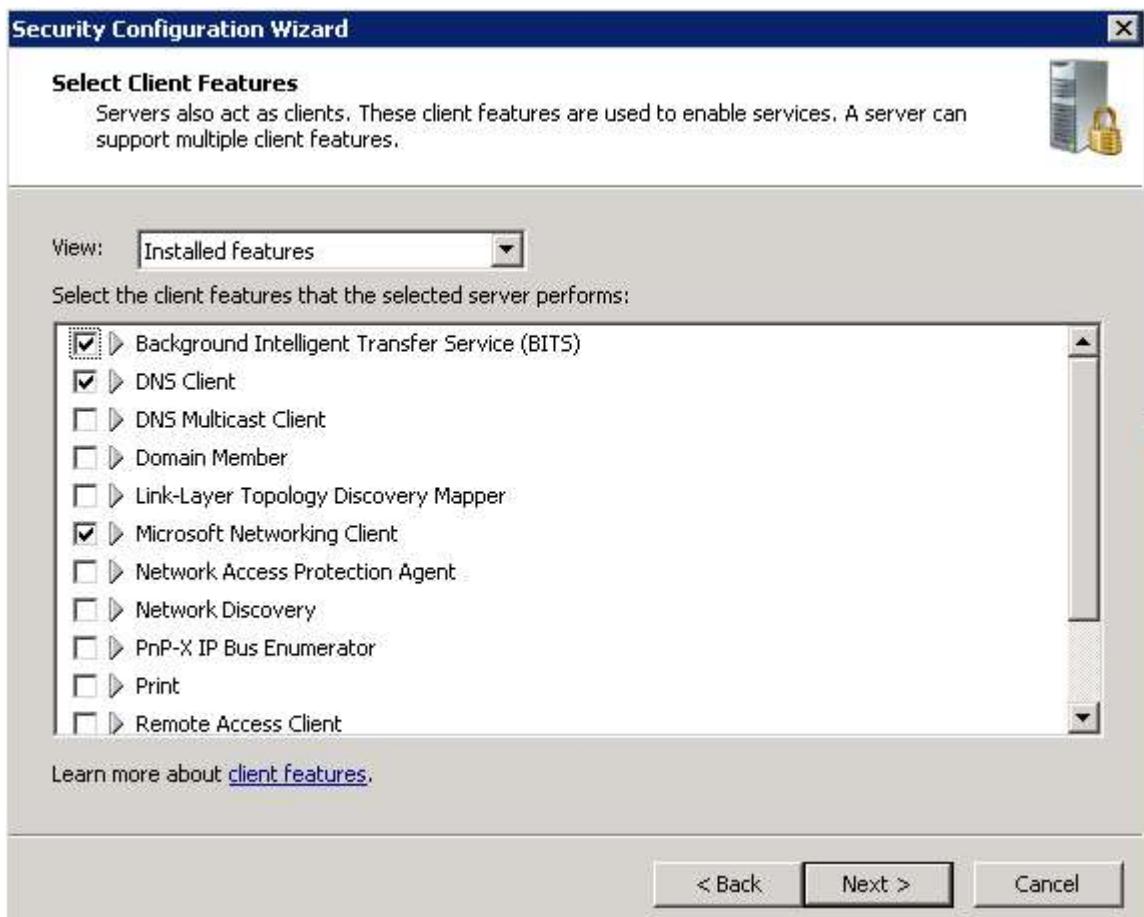


Next

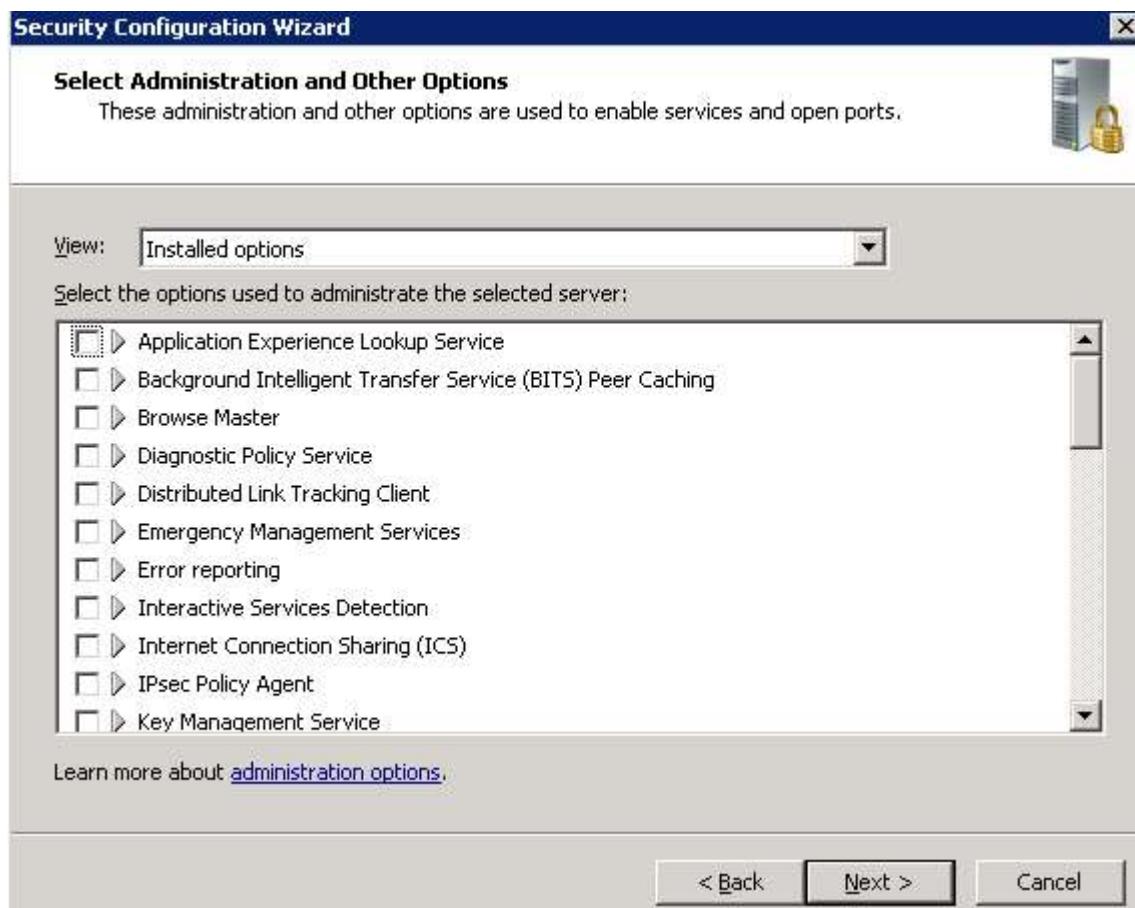


Uncheck all, except for 'Volume Shadow Copy', Next

Installed Features



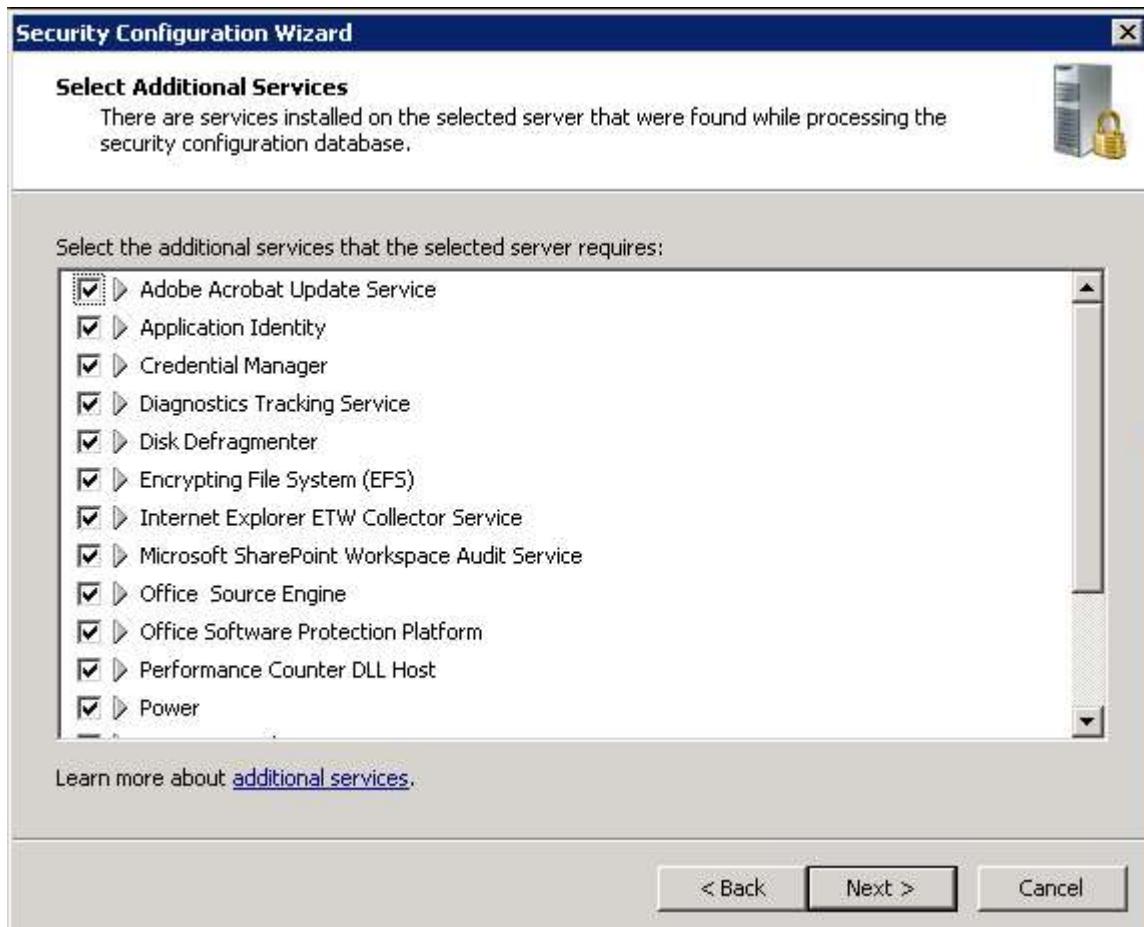
Uncheck all boxes except for Background Intelligent Transfer Service (BITS), DNS Client, Microsoft Networking Client, Time Synchronization, & Windows Update. Next



Make sure all boxes are unchecked except for Remote Desktop, if you are using Remote Desktop to connect to this system.

Important: If you are connecting to the system via VirtualBox or the VMware Player, you can also uncheck the box for Remote Desktop. Next

Additional services



Leave these boxes checked, Next



Leave the defaults, Next

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 Experience	Manual	Disabled	Application Experience
Application Layer Gateway S...	Manual	Disabled	Internet Connection Sh...
Application Management	Manual	Disabled	Application installation I...
AudioEndpointBuilder	Manual	Disabled	Windows Audio
audiosrv	Manual	Disabled	Windows Audio
Background Intelligent Transf...	Manual	Automatic	Background Intelligent
Certificate Propagation	Manual	Automatic	Smart Card

⚠ 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**

Next

Network Security

Security Configuration Wizard

Network Security

Use this section to configure rules for Windows Firewall with Advanced Security based on the roles and administrative options you selected.

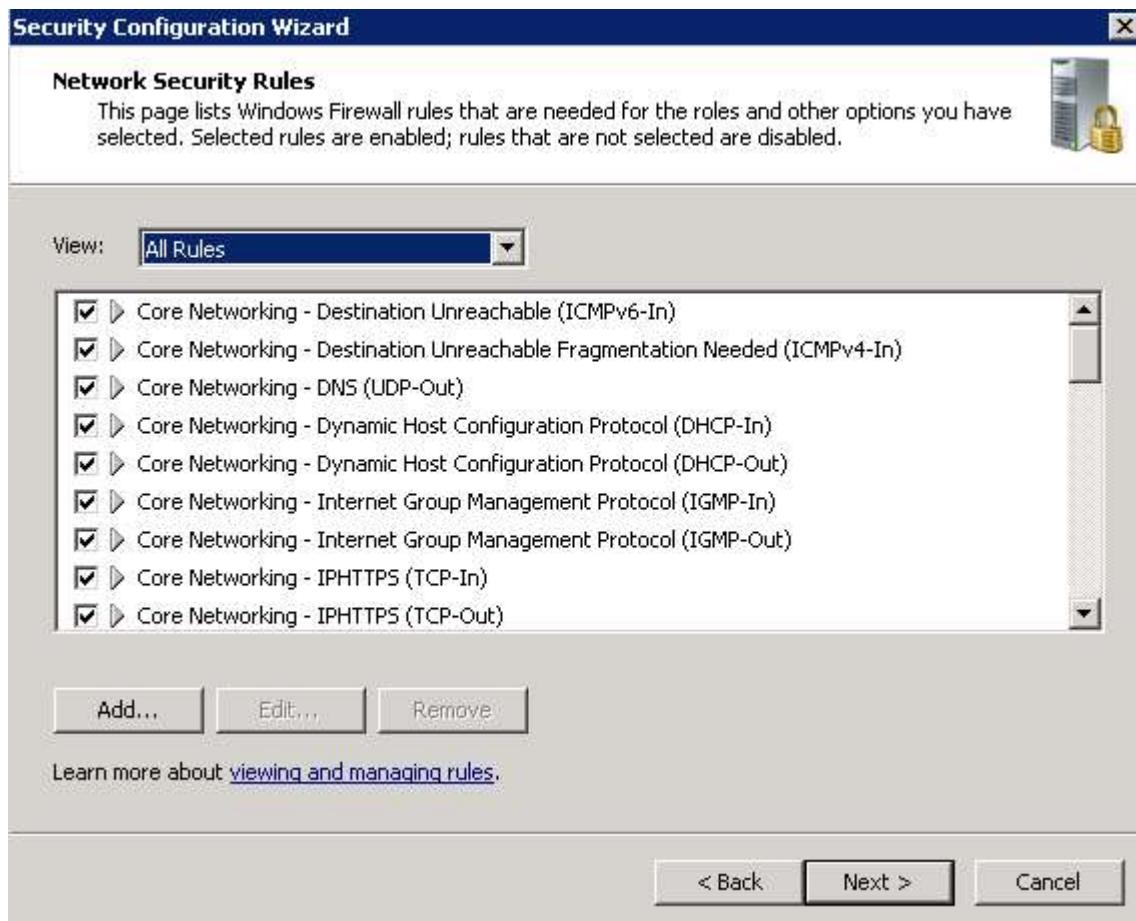
 Answering these questions incorrectly might prevent the selected server from communicating with other computers.

[Skip this section](#)
If you skip this section, this security policy will not contain firewall settings.

Learn more about [network security](#) and managing network security risk with SCW.

[< Back](#) [Next >](#) [Cancel](#)

Next



Leave all boxes checked, Next

Registry Settings

Security Configuration Wizard X

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.](#)

[< Back](#) [Next >](#) [Cancel](#)

Next

Require SMB Security Signatures

Security Configuration Wizard X

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.

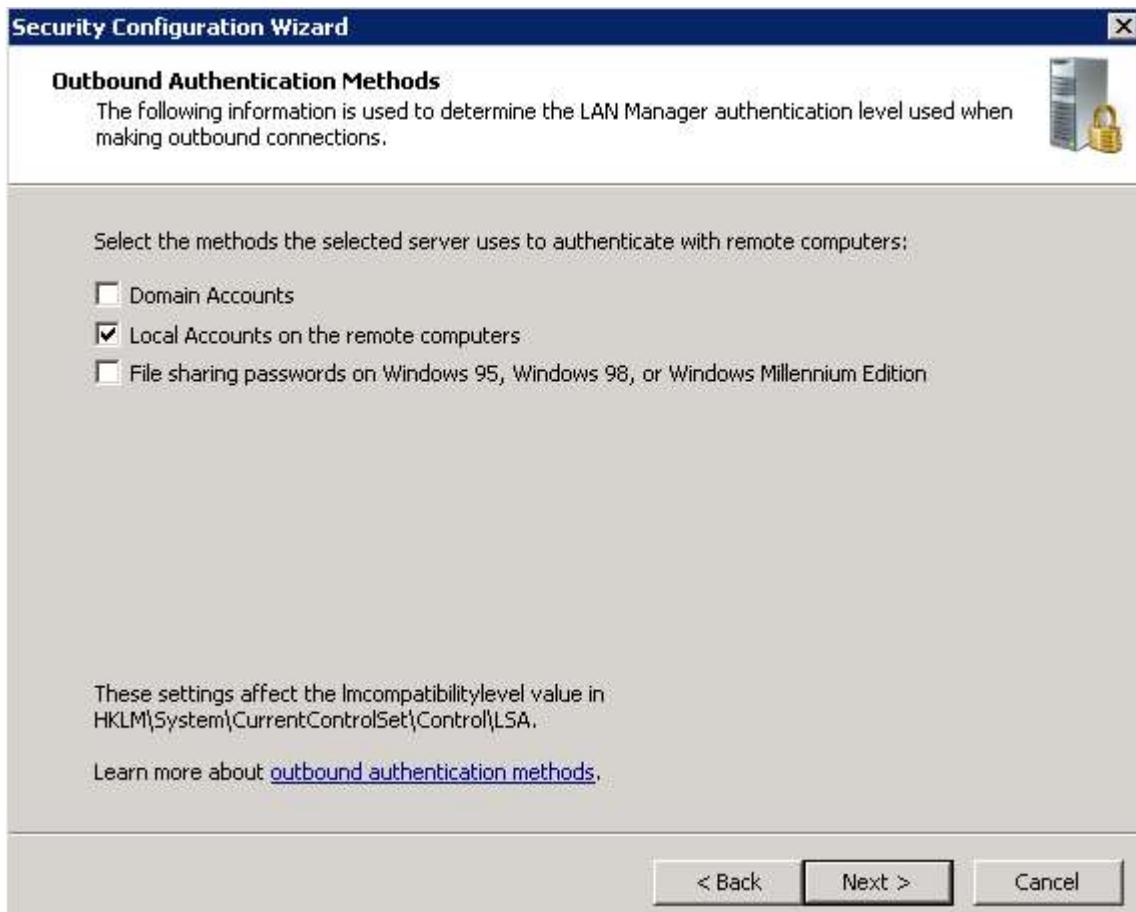
These settings affect the `RequireSecuritySignature` value in `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters`.

Learn more about [SMB security signatures](#).

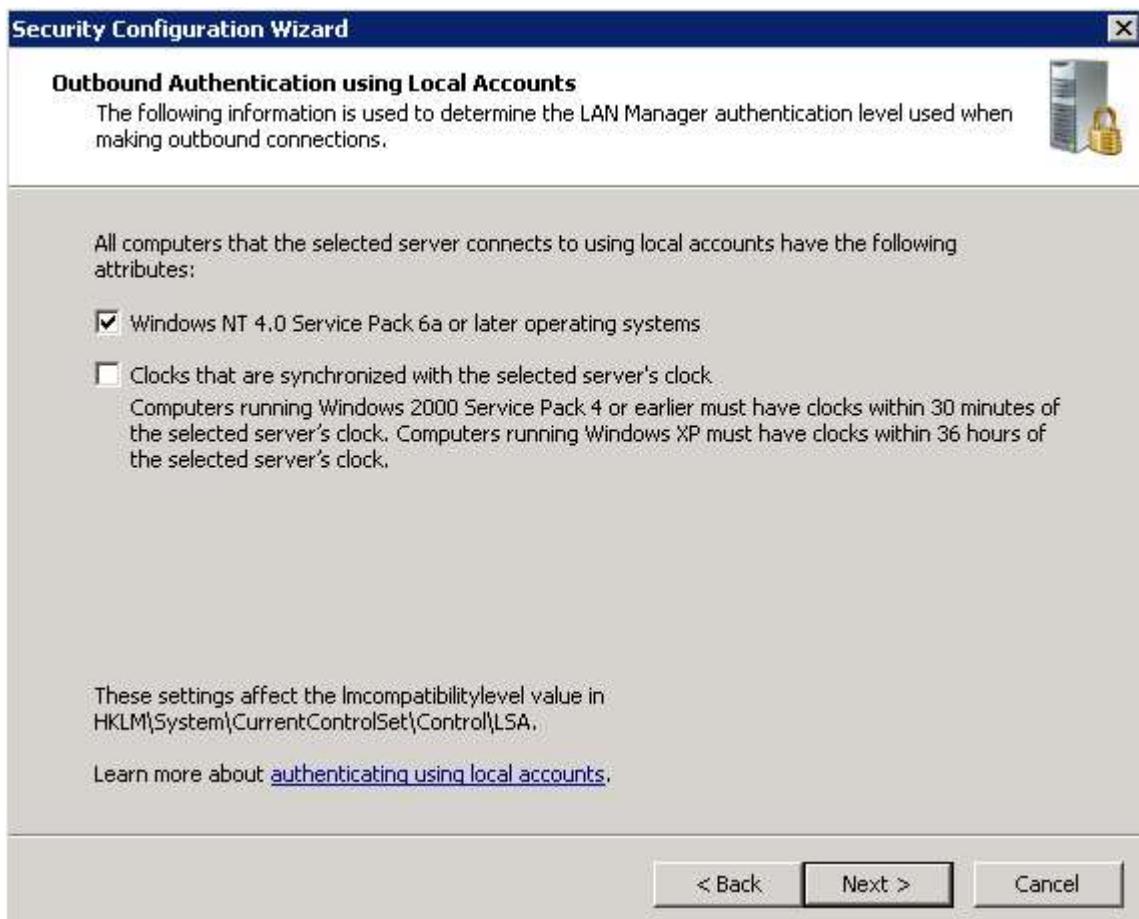
< Back Next > Cancel

Leave both boxes checked, Next

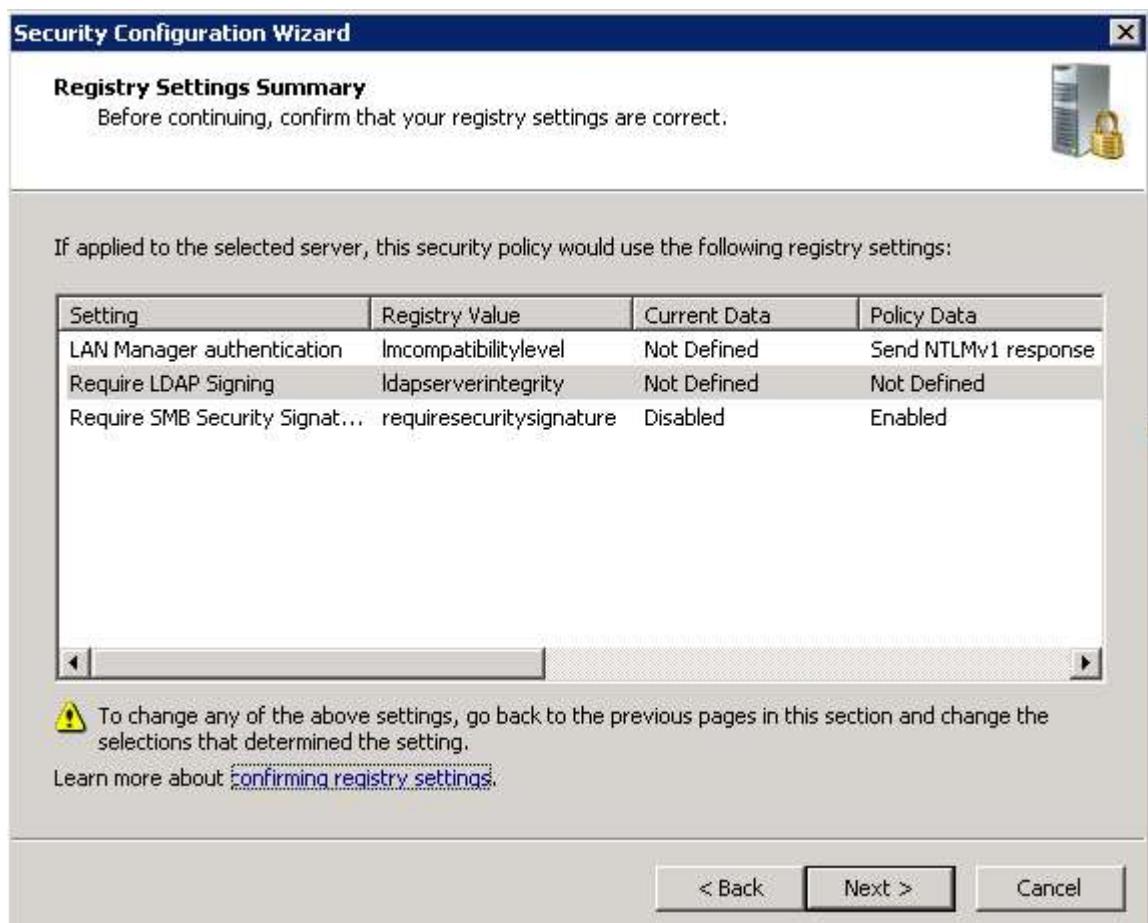
Outbound authentication methods



Check the box for Local Accounts on remote computers, Next



Leave the Windows NT 4.0 Service Pack 6a or later operating systems checked, Next



Next

Audit Policy

Security Configuration Wizard

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.

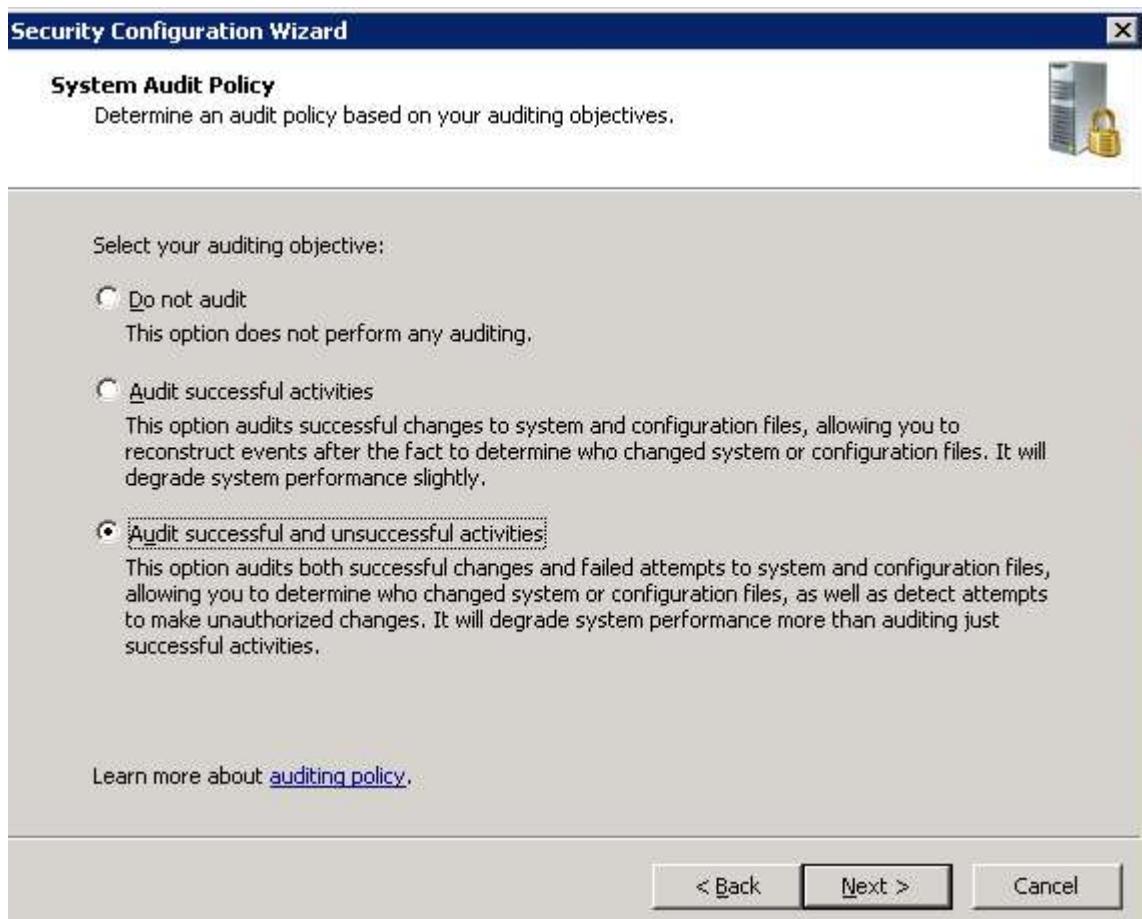
Skip this section
If you skip this section, this security policy will not configure auditing.

Learn more about [audit policy](#).

< Back **Next >** **Cancel**

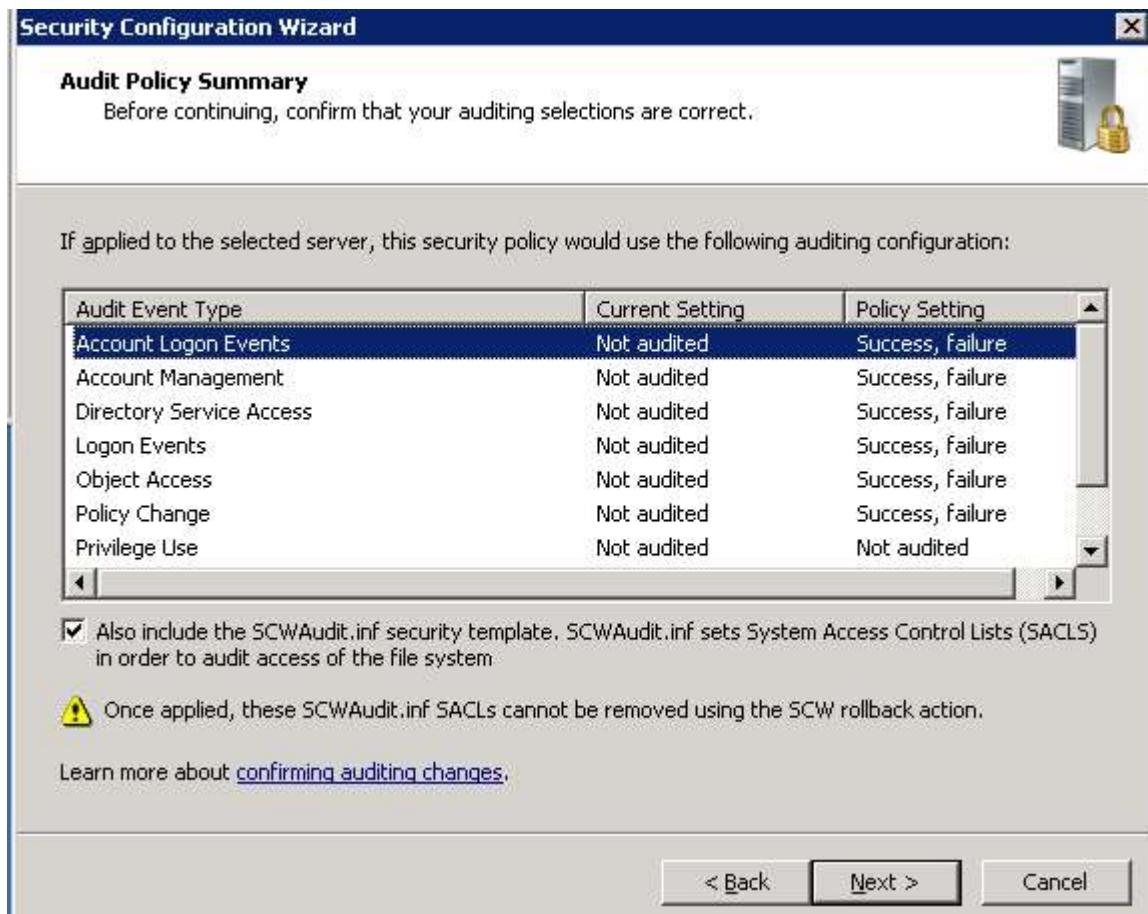
Next

System Audit Policy



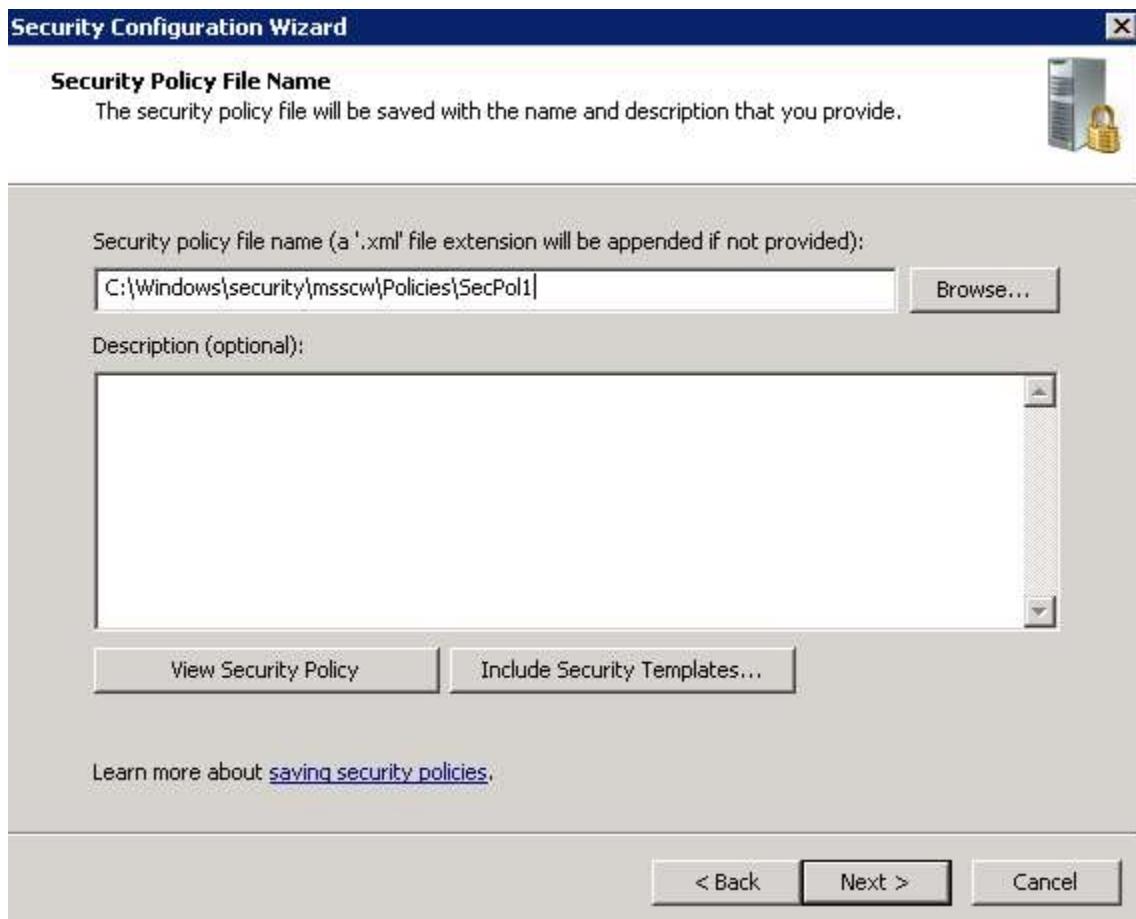
Select Audit successful and unsuccessful activities, Next

Audit Policy Summary



Next. Save Security Policy. Next

Security Policy File Name



Enter a name (I entered SecPol1), Next

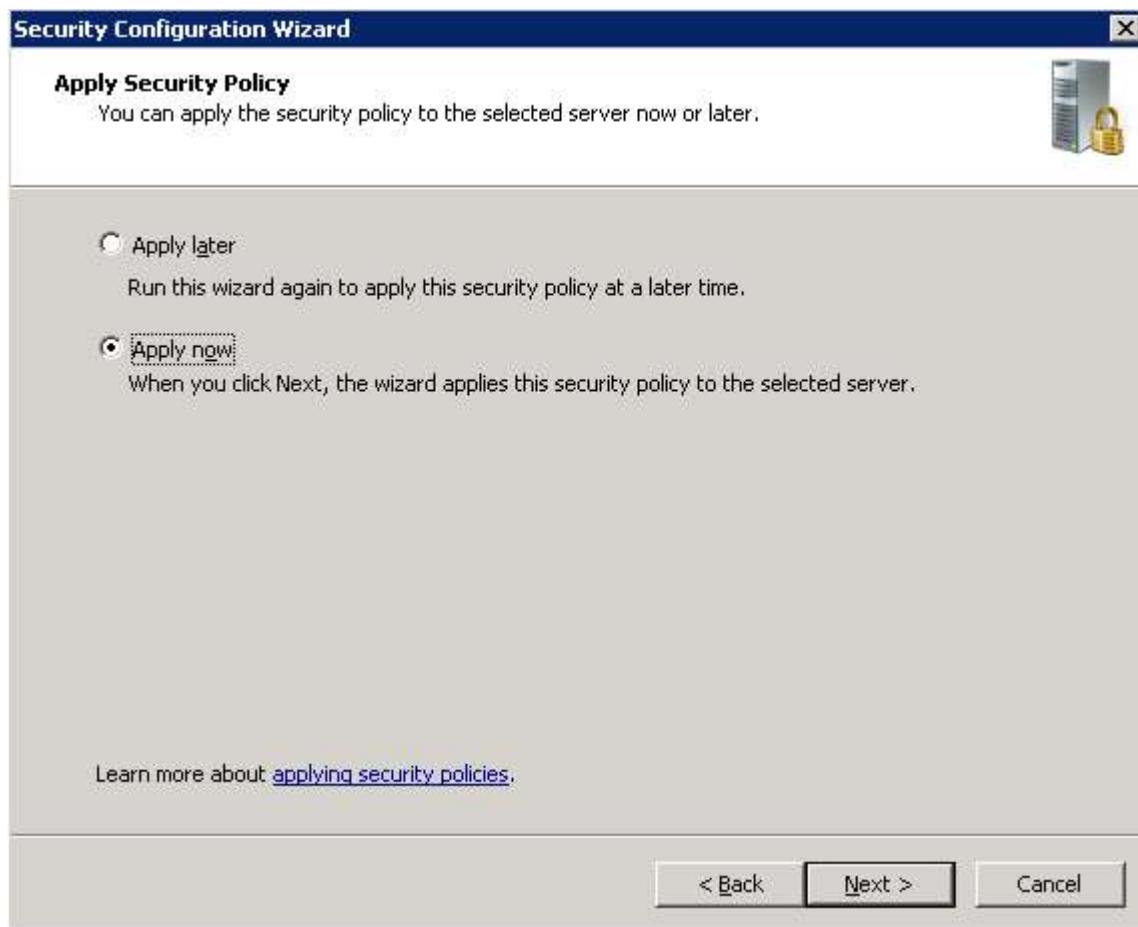
Apply Now, Next

It always seems to end with an Unspecified error



Finish

On review, it seems that the SCW worked, just ignore the error notice



Change to Apply now. Next

Type	Time	HRESULT	Message	System Error Message
Info	1/9/2018 1:18:38 PM	0	Starting engine operation: Configure	
Info	1/9/2018 1:18:38 PM	0	XML security policy is C:\Windows\security\msscw\Logs\Policy.xml	
Extension Name Microsoft.OS.SCETemplates				
Info	1/9/2018 1:18:38 PM	0	Configuration started	
Info	1/9/2018 1:19:36 PM	0	Configuration ended	
Extension Name Microsoft.OS.Services				
Info	1/9/2018 1:19:36 PM	0	Configuration started	
Error	1/9/2018 1:20:10 PM	0x80070005	Error configuring C:\Windows\security\msscw\ConfigureFiles\Services.inf	Access is denied.
Info	1/9/2018 1:20:10 PM	0x80070005	Configuration ended	Access is denied.
Error	1/9/2018 1:20:10 PM	0x80070005	Cannot complete extension processing: Microsoft.OS.Services	Access is denied.
Extension Name Microsoft.OS.Networking.Firewall				
Info	1/9/2018 1:20:10 PM	0	Configuration started	
Info	1/9/2018 1:20:10 PM	0	Succeeded to parse the XML security policy	
Info	1/9/2018 1:20:11 PM	0	Succeeded to enforce the security policy to the Windows Firewall	
Info	1/9/2018 1:20:11 PM	0	Configuration ended	
Extension Name Microsoft.OS.Registry.Values				
Info	1/9/2018 1:20:11 PM	0	Configuration started	
Info	1/9/2018 1:20:11 PM	0	Configuration ended	
Extension Name Microsoft.OS.Audit				
Info	1/9/2018 1:20:11 PM	0	Configuration started	
Info	1/9/2018 1:20:11 PM	0	Configuration ended	