Microsoft SCW (Security Configuration Wizard)

About the SCW

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

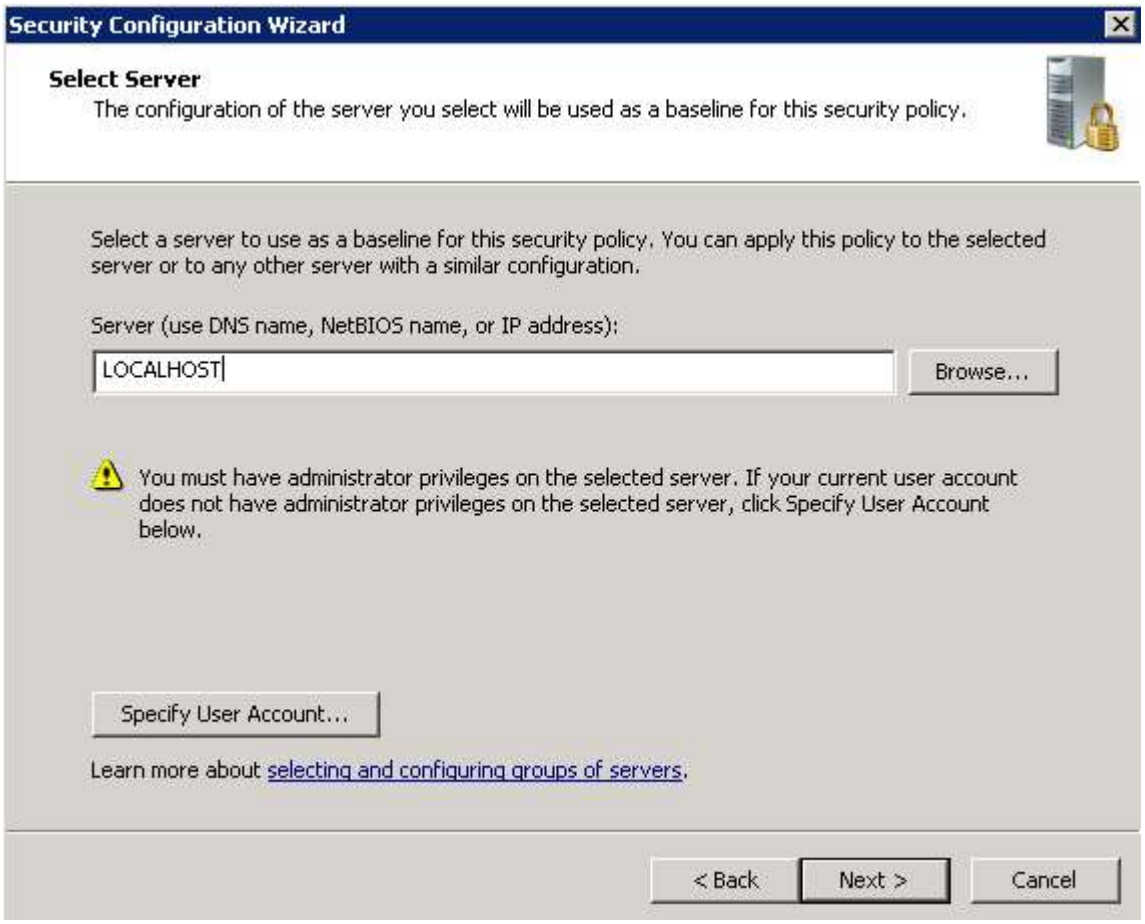
Removes unused firewall rules based on Server Roles

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

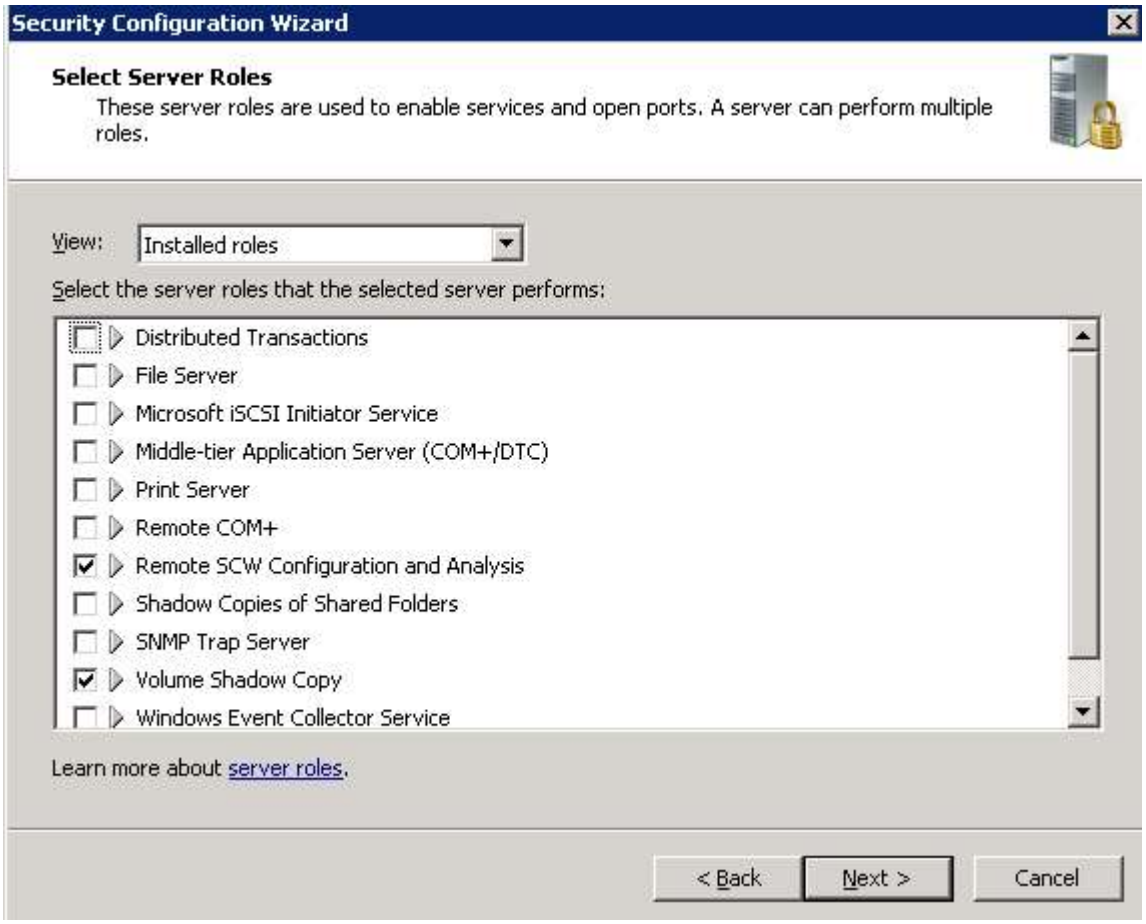


Enter hostname or LOCALHOST (to identify the computers' hostname, you can type hostname at an Administrator Command Prompt), Next

Processing Complete, Next

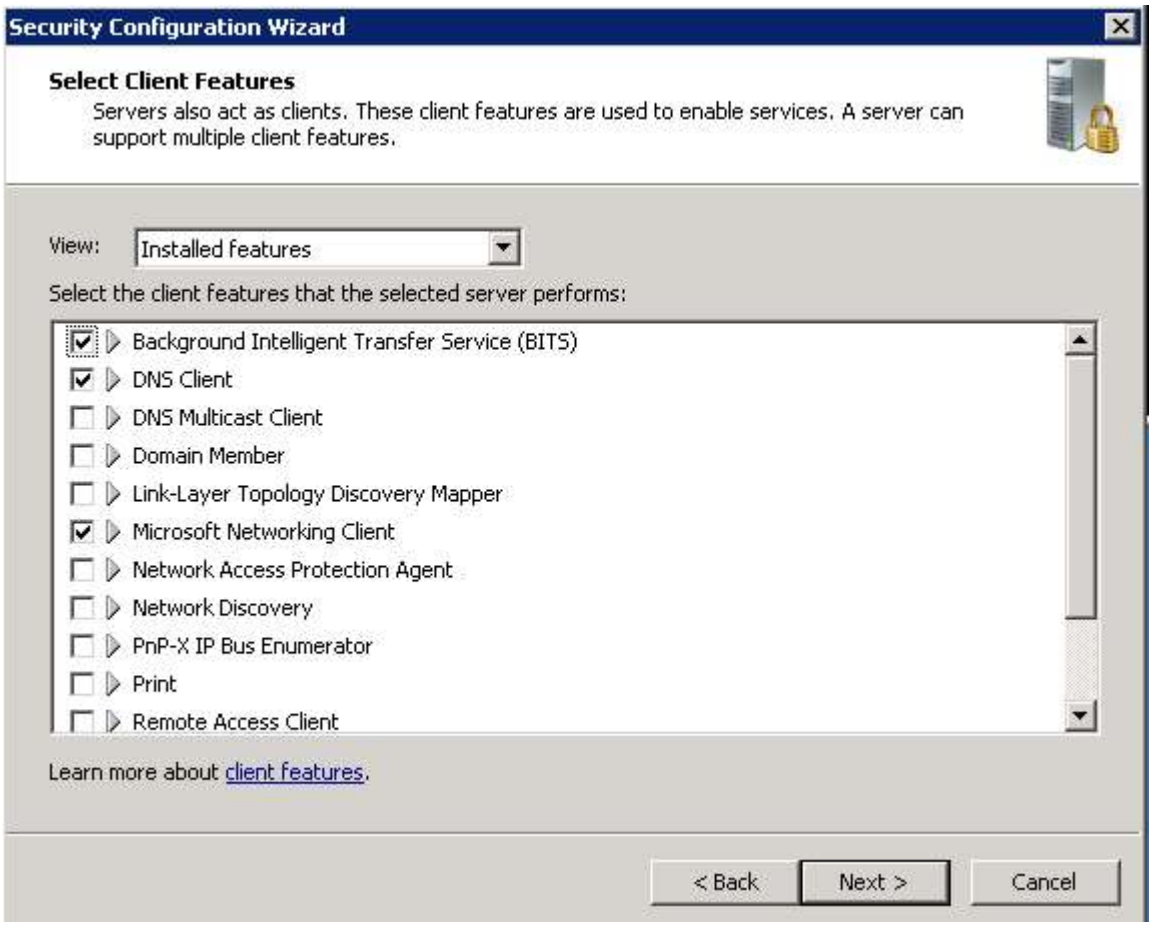

Security Configuration Wizard
Role-Based Service Configuration
Use this section to configure services based on the selected server's roles and other features. These roles and other features are also used to determine settings in other sections.
Answering these questions incorrectly might disable desired functionality or enable undesired functionality. Before proceeding, make sure that you have thorough knowledge of the roles and other features performed by this server.
Learn more about configuring services based on roles.
< Back
Next >
Cancel

Next

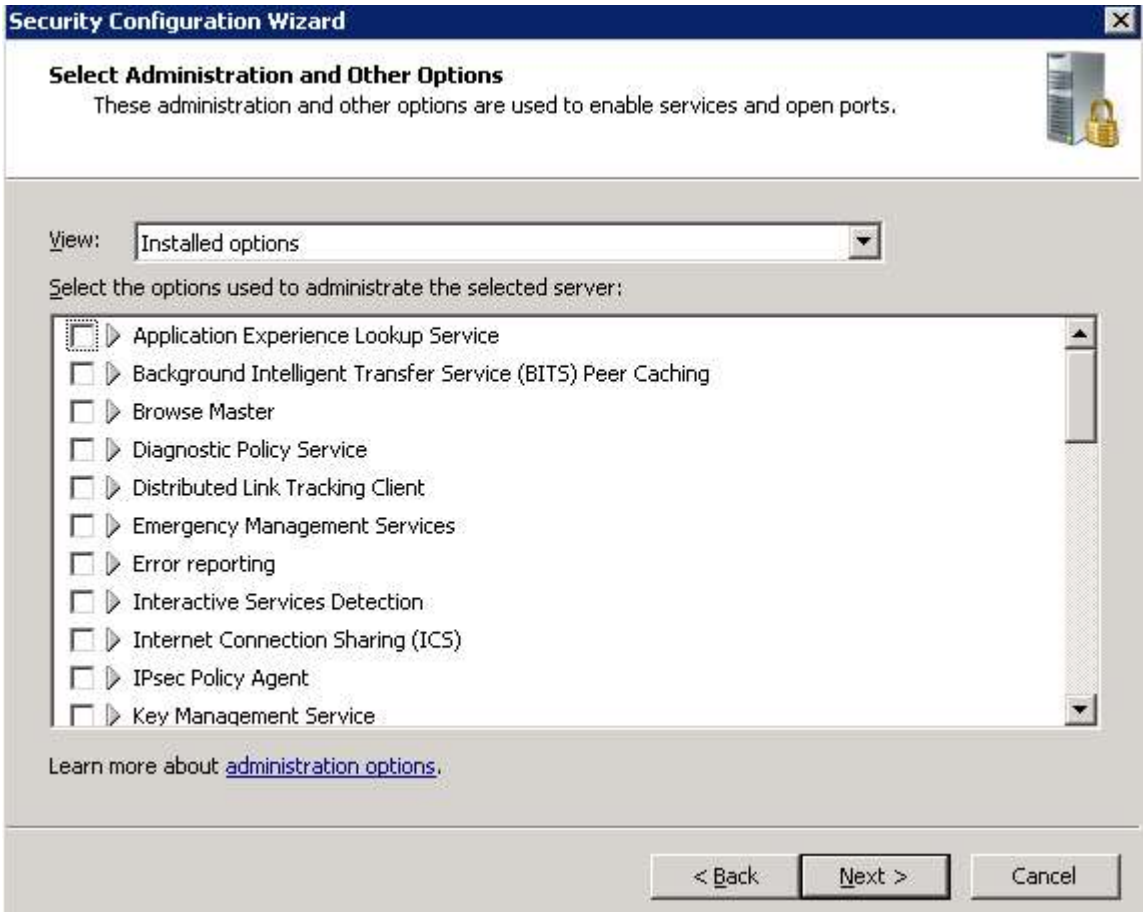


Uncheck all, except for 'Volume Shadow Copy', Next

Installed Features



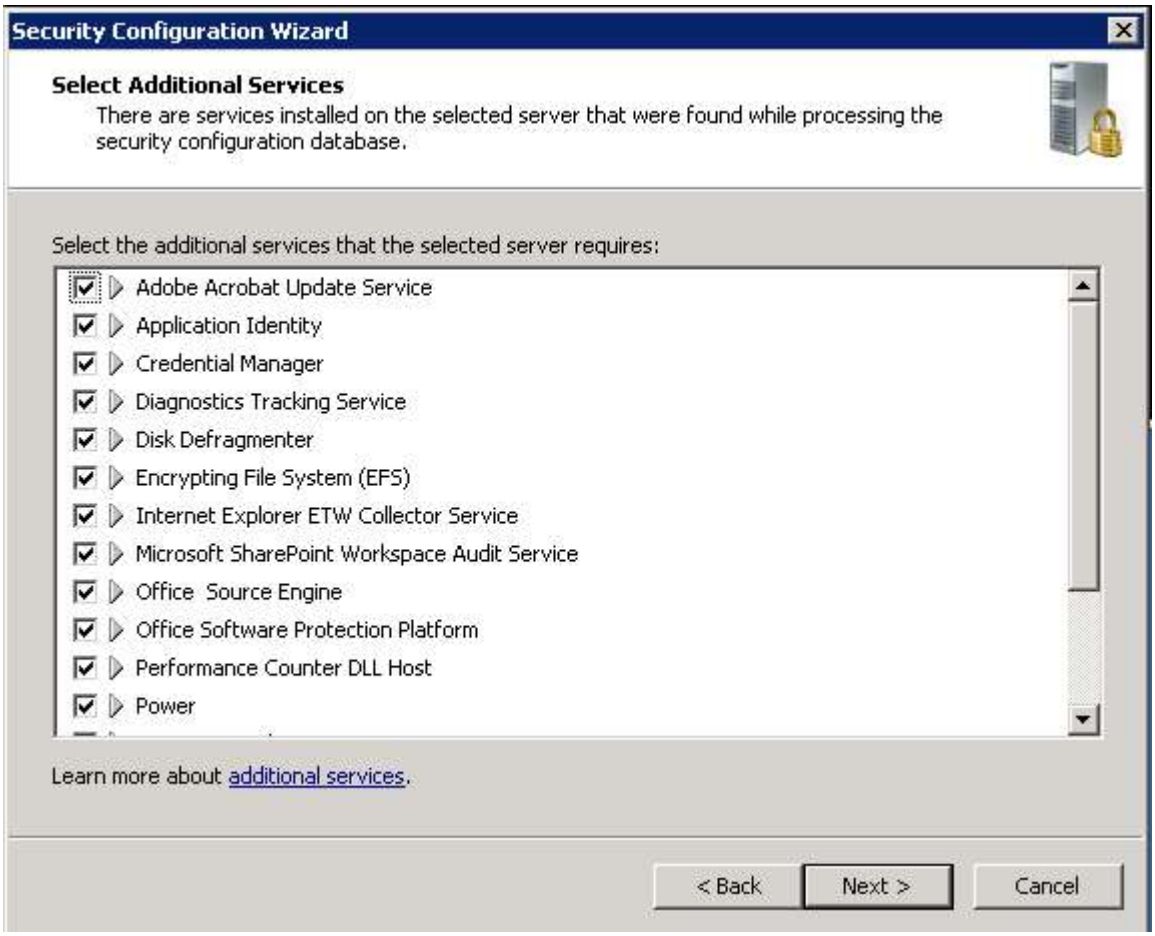
Uncheck all boxes except for Background Intelligent Transfer Service (BITS), DNS Client, Microsoft Networking Client, Time Synchronization, & Windows Update. Next



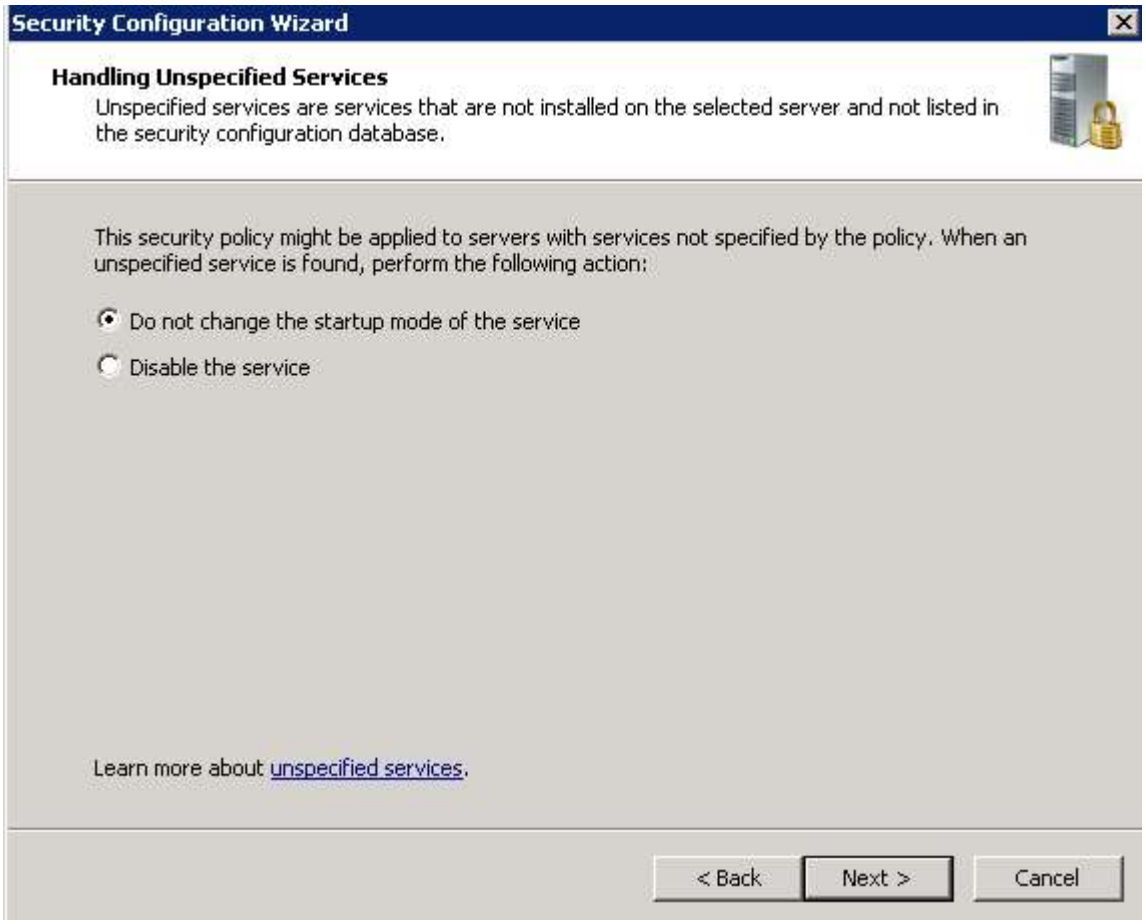
Make sure all boxes are unchecked except for Remote Desktop, if you are using Remote Desktop to connect to this system.

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

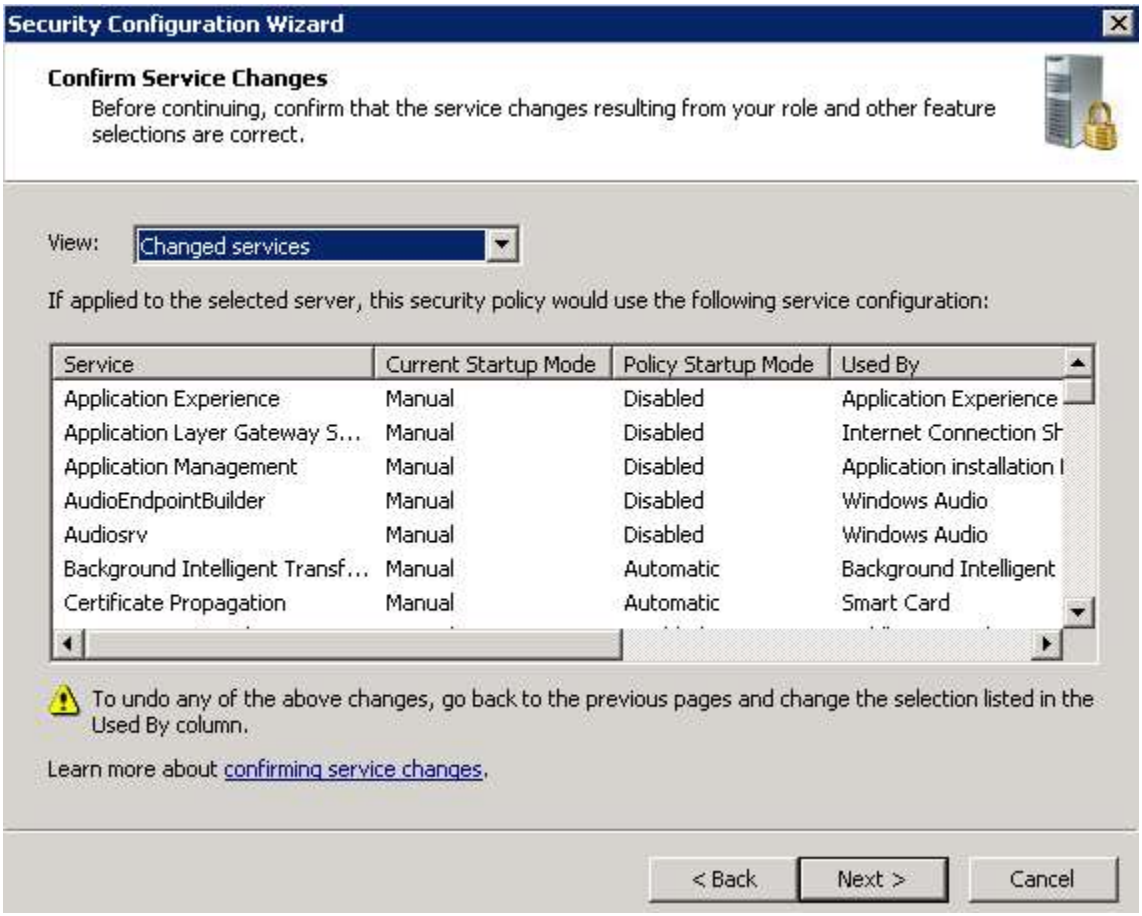
Additional services



Leave these boxes checked, Next



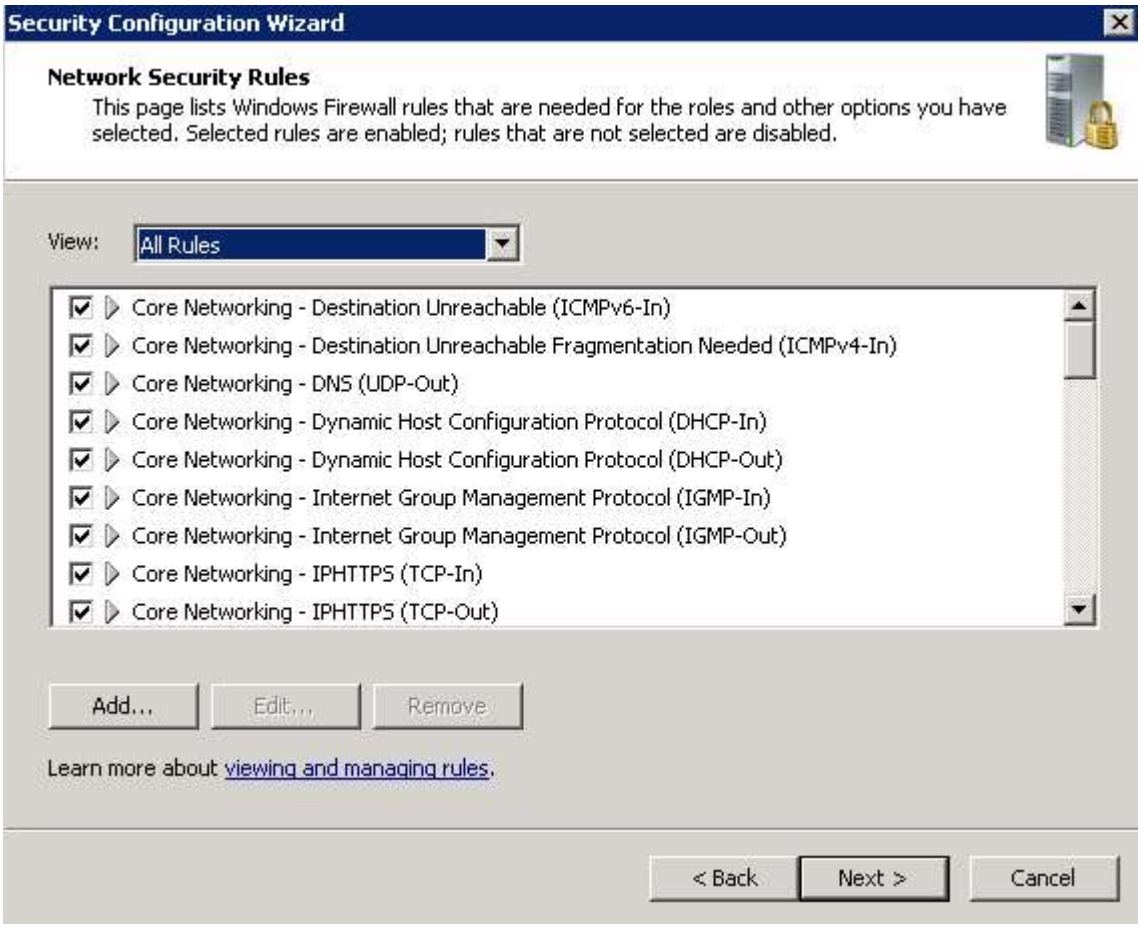
Leave the defaults, Next


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

Next

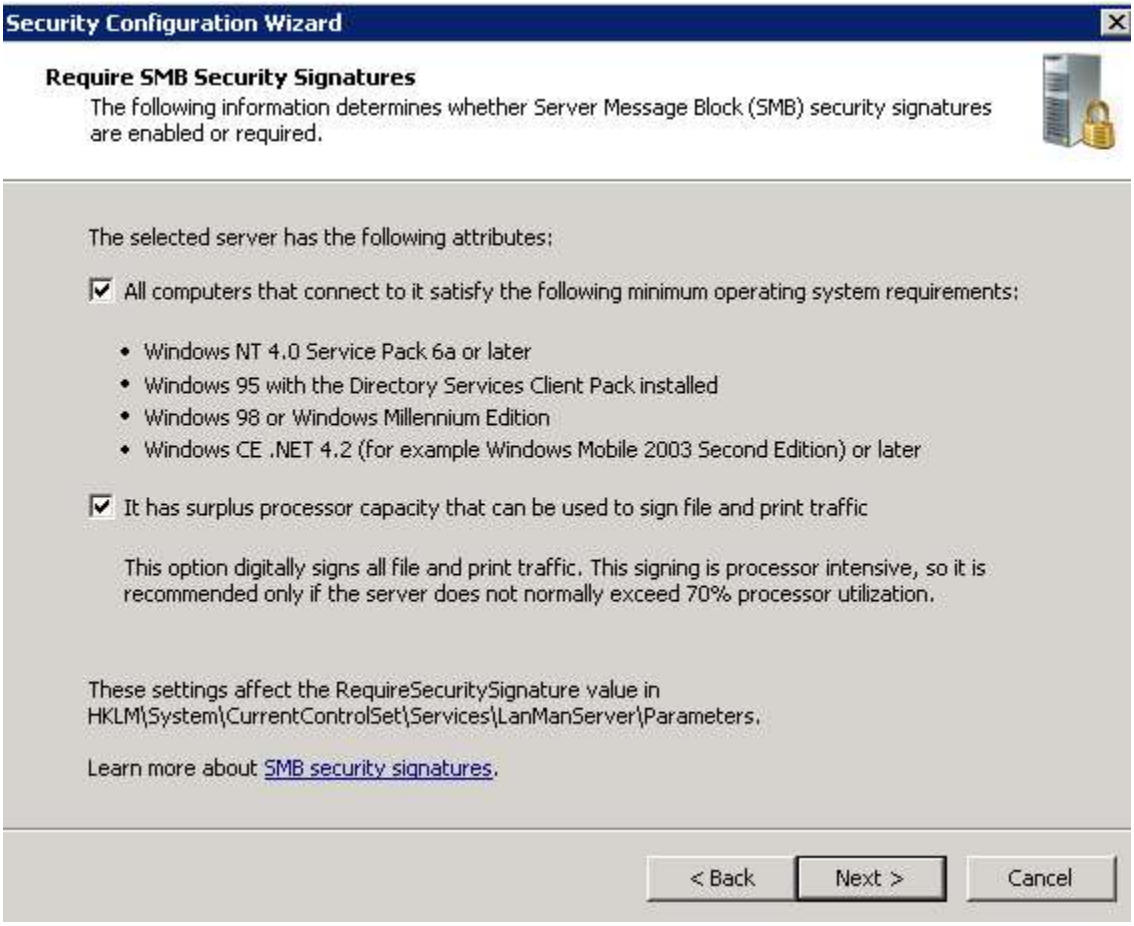


Leave all boxes checked, Next

Registry Settings

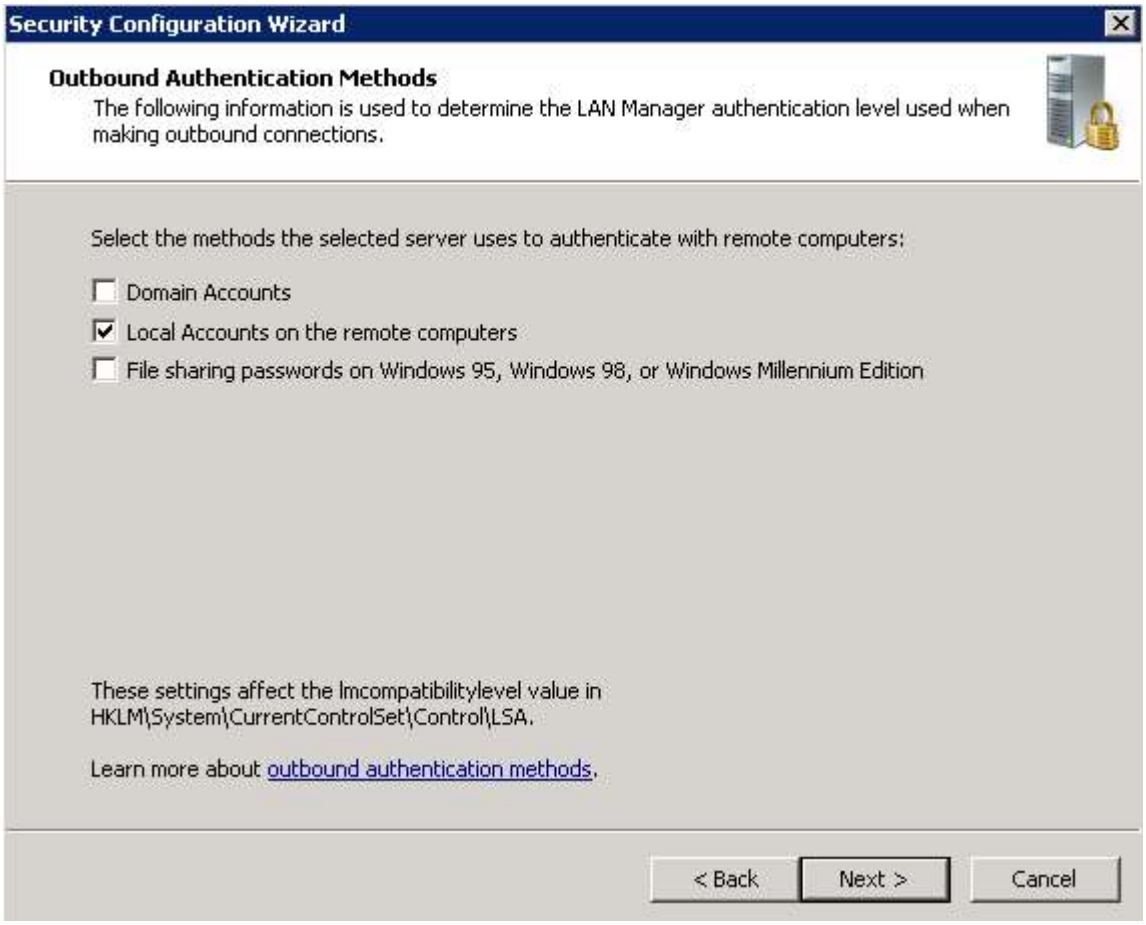
Next

Require SMB Security Signatures



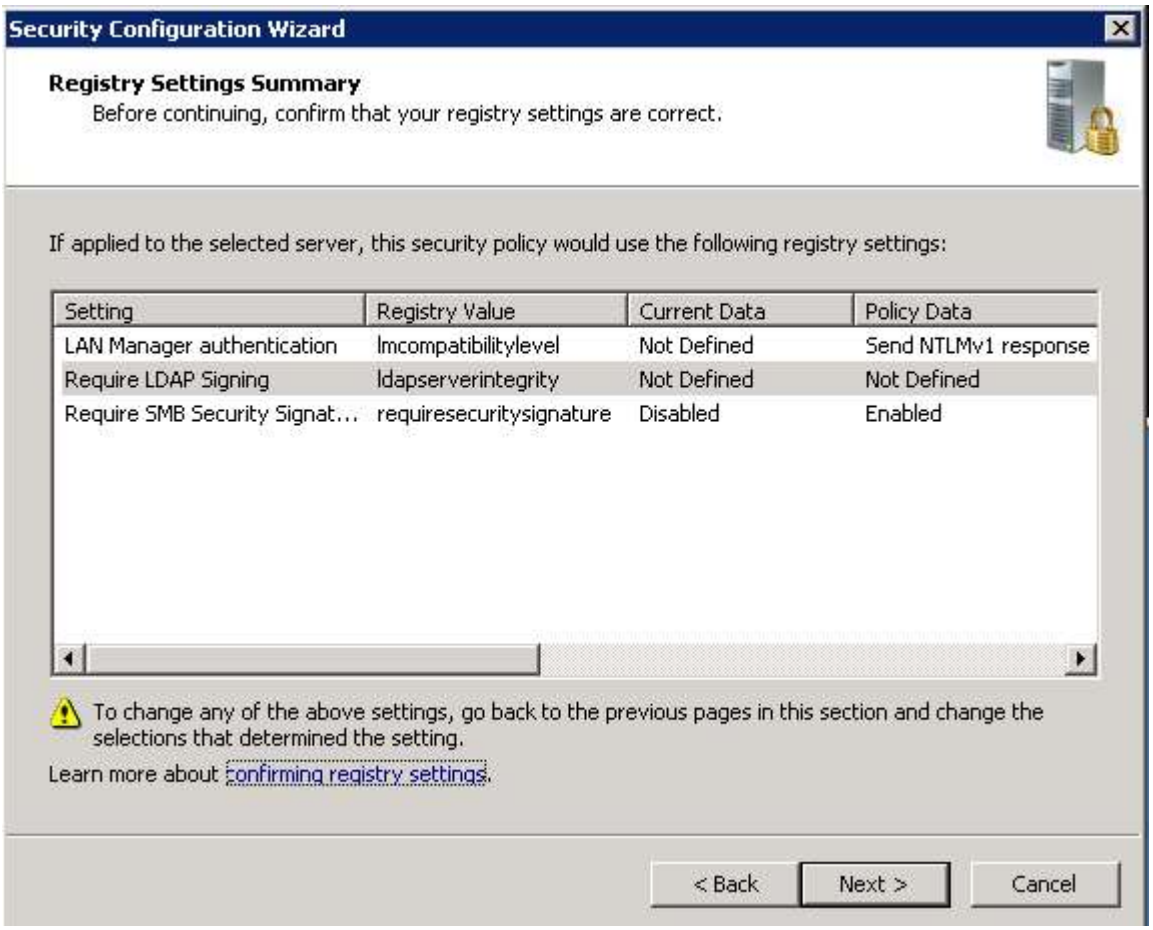
Leave both boxes checked, Next

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

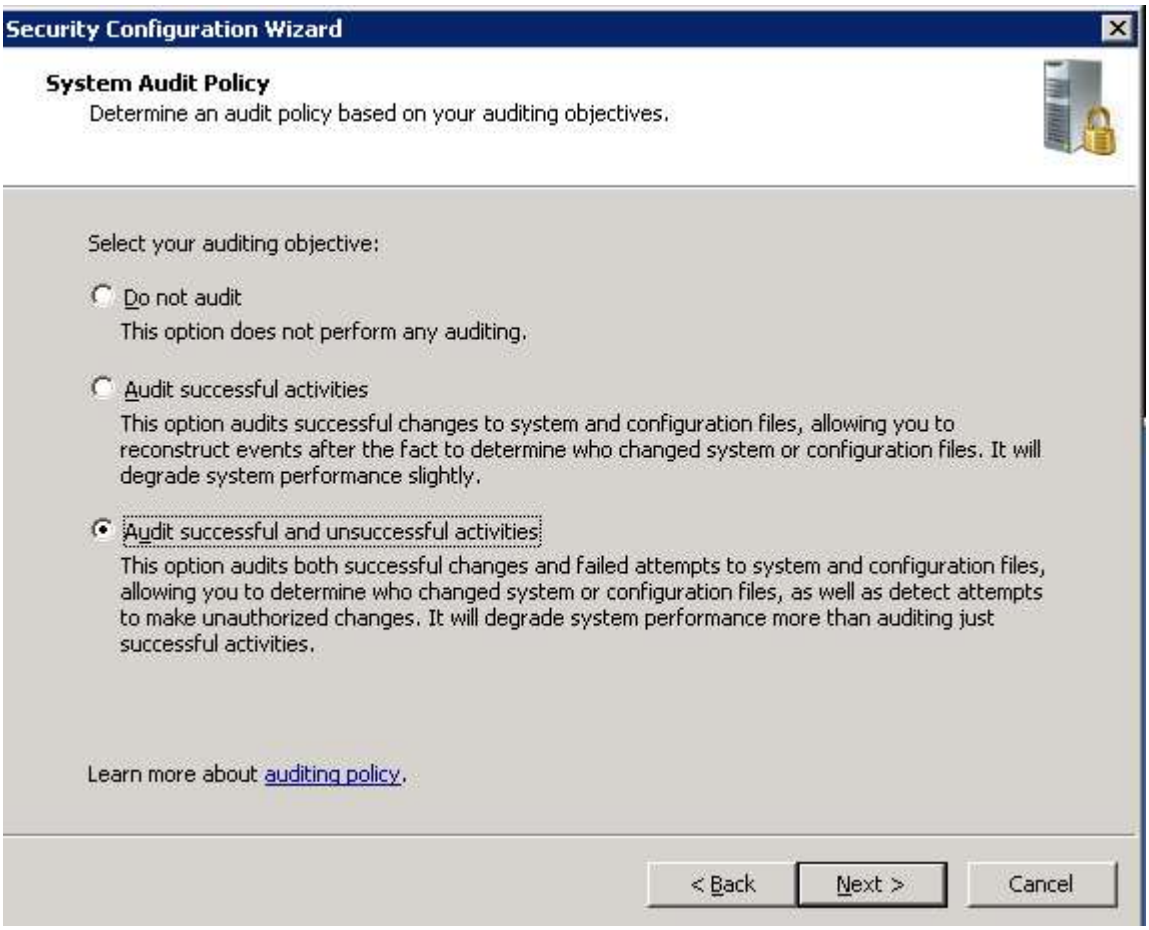


Next

Audit Policy

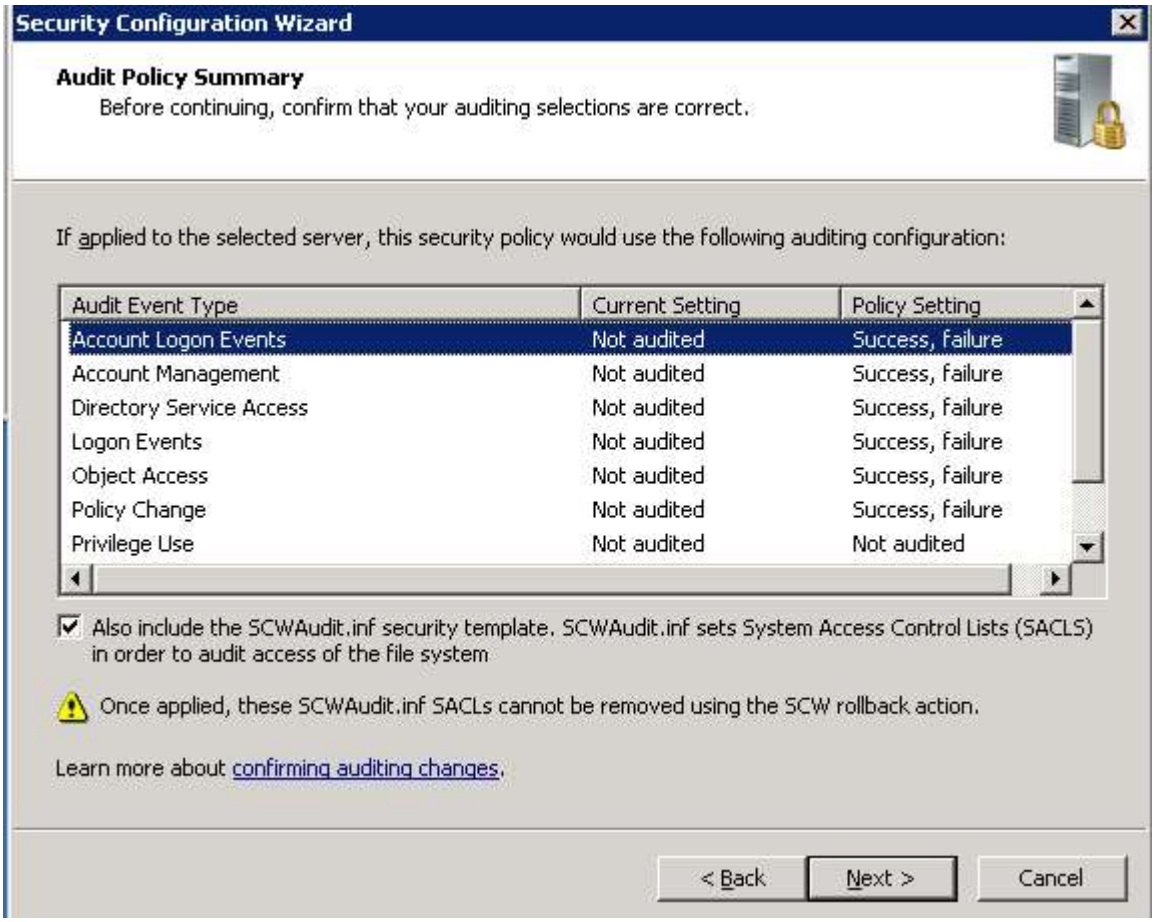
Next

System Audit Policy



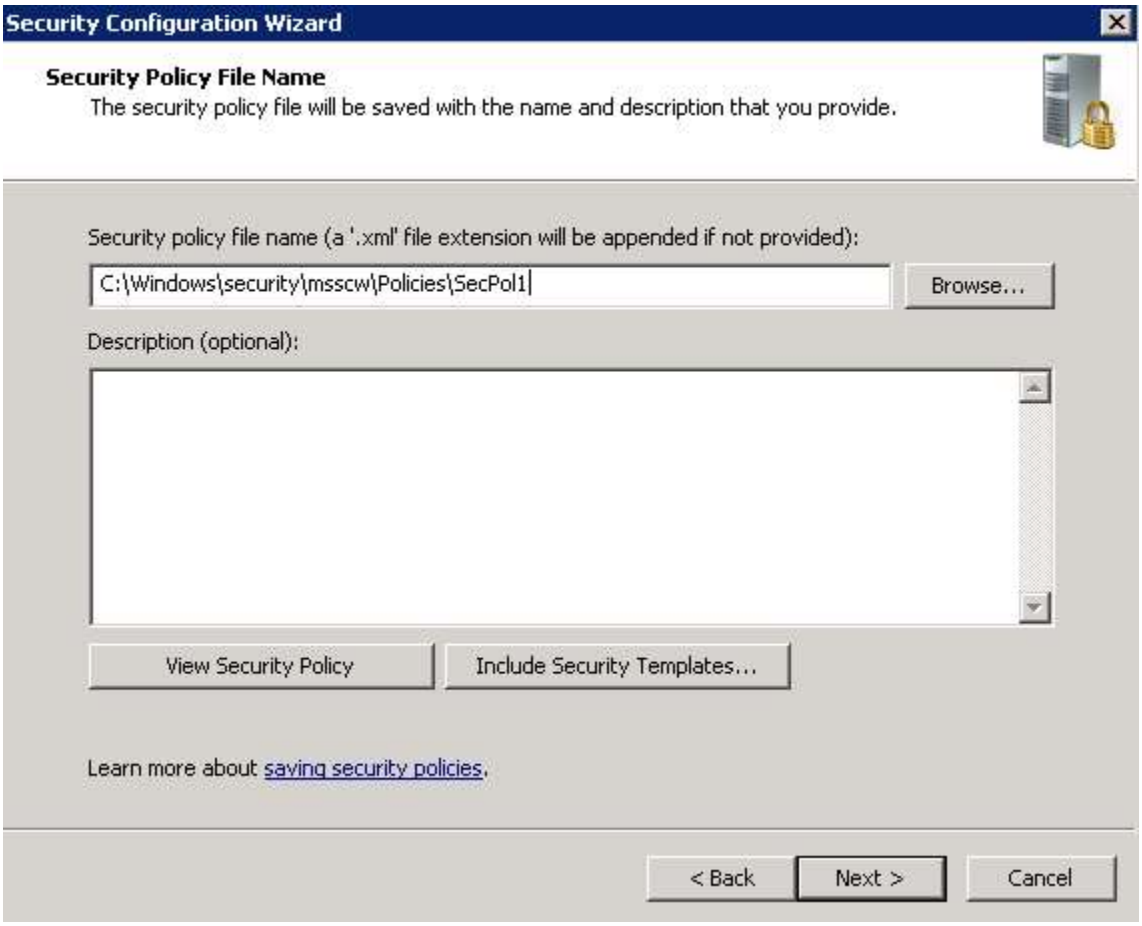
Select Audit successful and unsuccessful activities, Next

Audit Policy Summary



Next. Save Security Policy. Next

Security Policy File Name



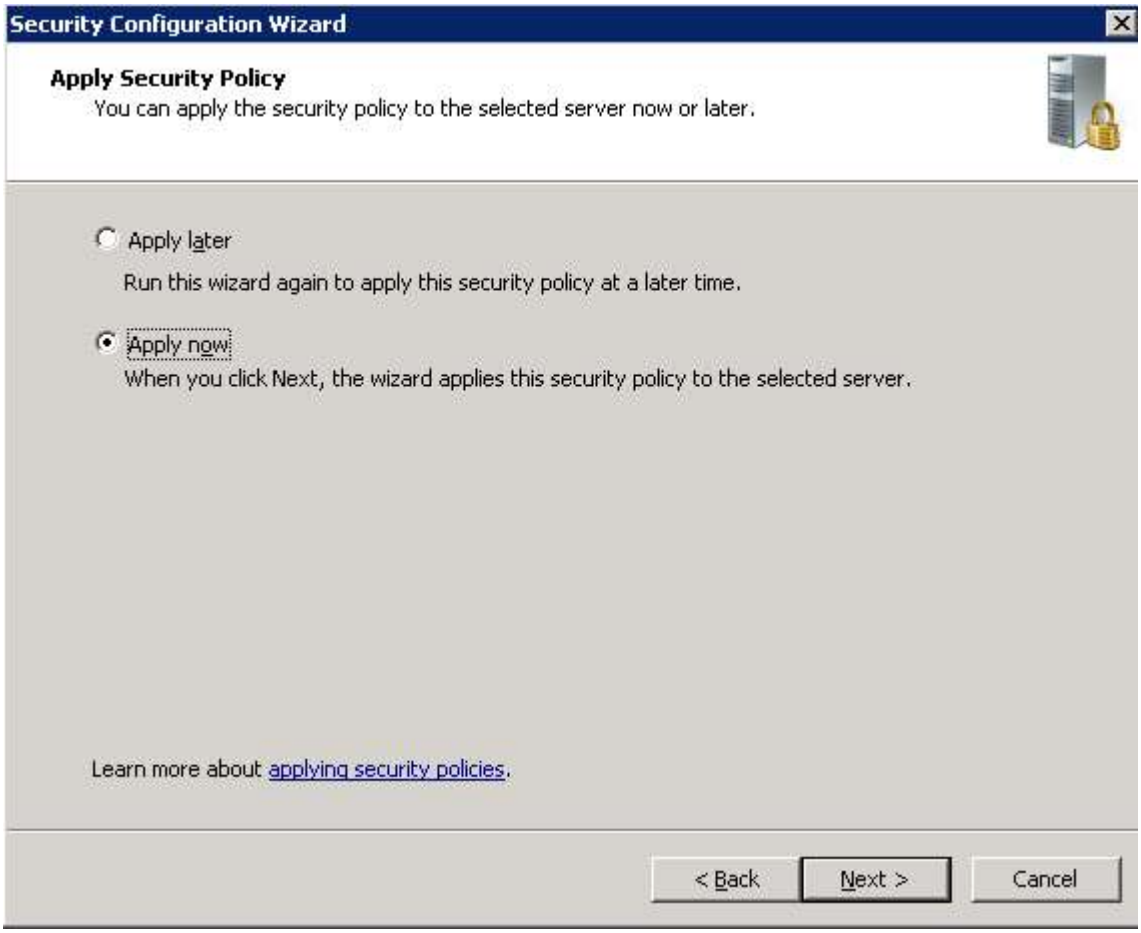
Enter a name (I entered SecPol1), Next

Apply Now, Next

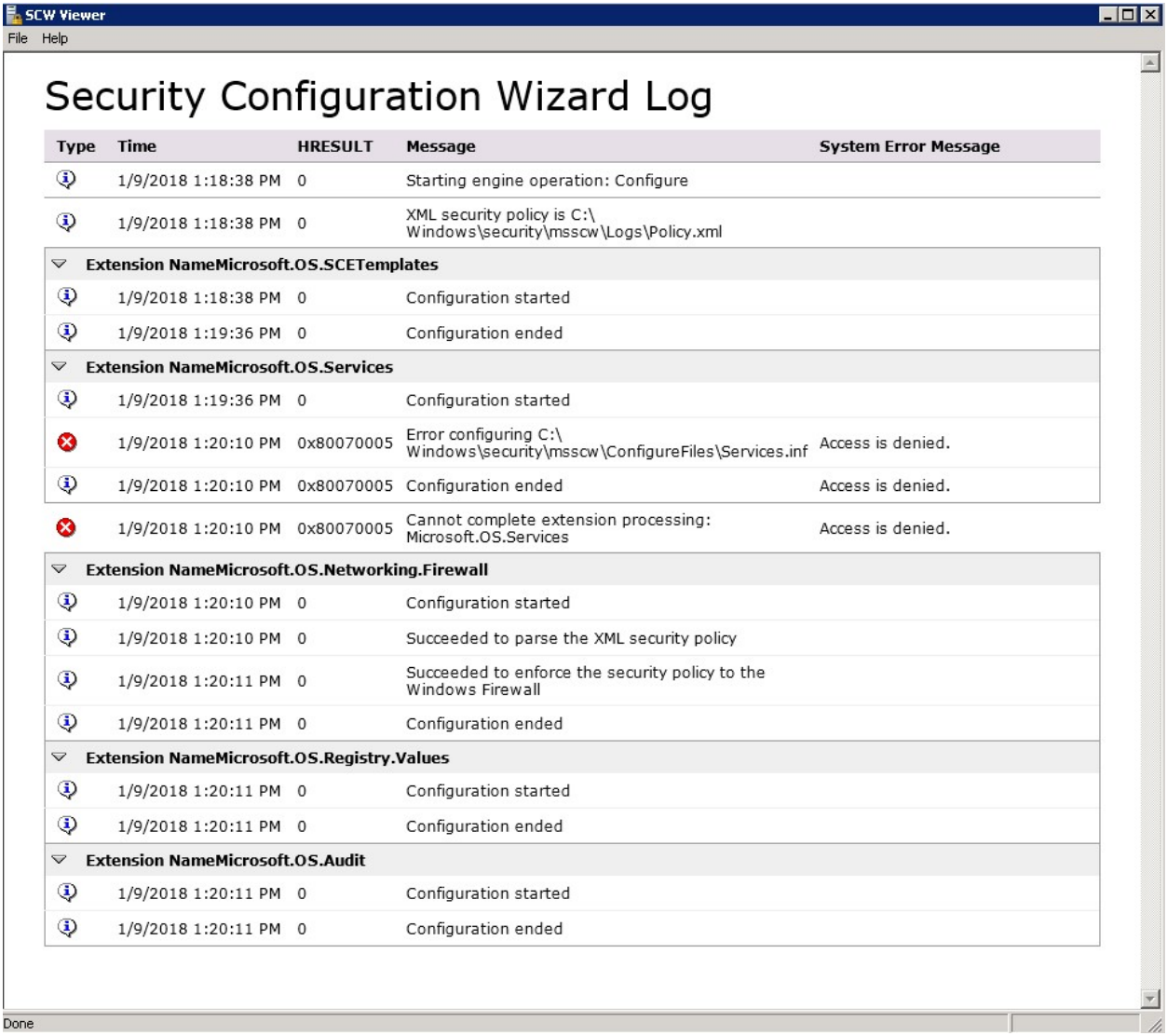
It always seems to end with an Unspecified error

Finish

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



Change to Apply now. Next


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