IP Office Technical Tip

Tip no: 119

Release Date: 20 Jan 2006

Region: GLOBAL

Avaya IP Office Compact Contact Center (CCC) Security Modifications Post Windows 2003 SP1

Overview

In Microsoft Windows Server 2003 Service Pack 1, Microsoft is introducing a set of security technologies that will help to improve the ability of computers running Windows Server 2003 to withstand malicious attacks from viruses and worms. Changes have been made to DCOM, Windows security policy and various integrated components. Microsoft has also introduced a new tool to help manage server security policy called the Security Configuration Wizard (SCW).

Microsoft has posted a white paper that reviews 2003 Server SP1 functionality changes:

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

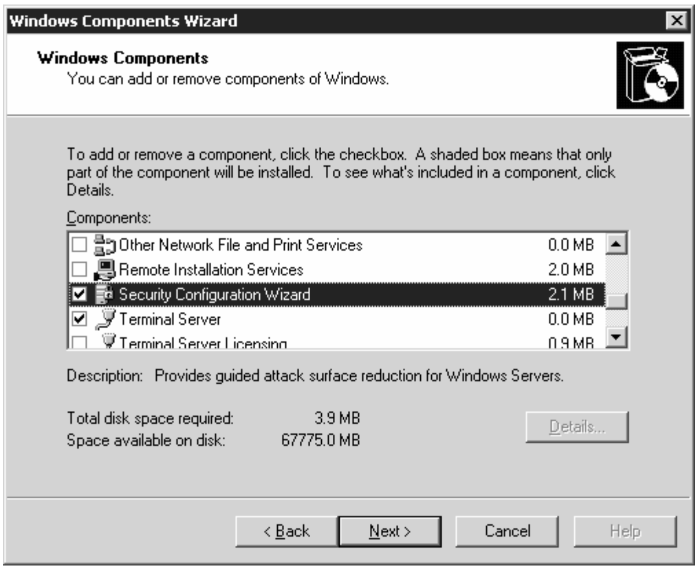
The security policy enforced by SP1 requires modifications in order for the IP Office Compact Contact Center (CCC) suite of client/server applications to work properly and maintain functionality. This document will cover the post Windows Server 2003 Service Pack 1 modifications needed for IP Office CCC.

After SP1 install – install SCW

Once SP1 has been installed, it is necessary to run the security configuration wizard:

Start / Settings / Control Panel / Add/Remove Programs / Add/Remove Windows Components

Scroll down and select Security Configuration Wizard – then select 'Next':



Windows Components

You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

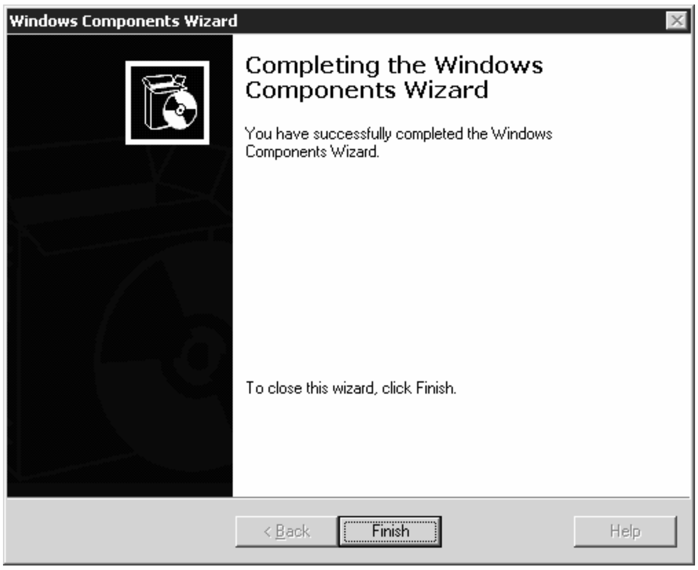
Components:

□	Other Network File and Print Services	0.0 MB
□	Remote Installation Services	2.0 MB
☑	Security Configuration Wizard	2.1 MB
☑	Terminal Server	0.0 MB
□	Terminal Server Licensing	0.9 MB

Description: Provides guided attack surface reduction for Windows Servers.

Total disk space required: 3.9 MB

Space available on disk: 67775.0 MB



Completing the Windows Components Wizard

You have successfully completed the Windows Components Wizard.

To close this wizard, click Finish.

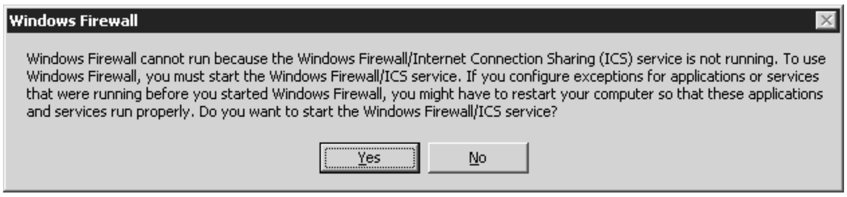
Click ‘Finish’ when complete.

Initialize Firewall

Once the Security Configuration Wizard has run, Windows Firewall needs to be started:

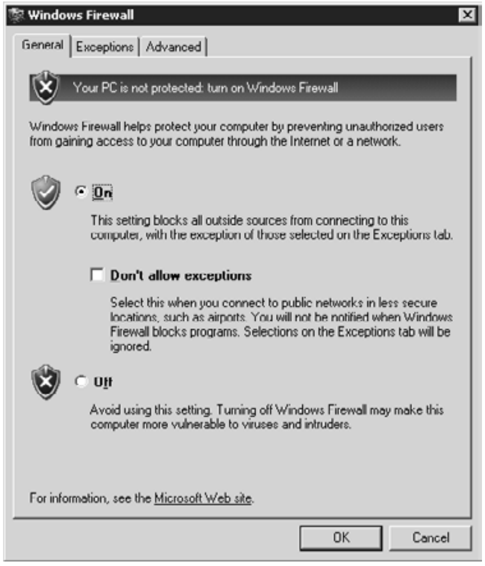
Start / Settings / Network Connections / Local Area Connection / Properties / Advanced Tab / Settings for Windows Firewall

The following confirmation prompt is displayed:



Windows Firewall cannot run because the Windows Firewall/Internet Connection Sharing (ICS) service is not running. To use Windows Firewall, you must start the Windows Firewall/ICS service. If you configure exceptions for applications or services that were running before you started Windows Firewall, you might have to restart your computer so that these applications and services run properly. Do you want to start the Windows Firewall/ICS service?

Select 'Yes' to turn the Firewall on:



Your PC is not protected: turn on Windows Firewall

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

● On

This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

□ Don't allow exceptions

Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.

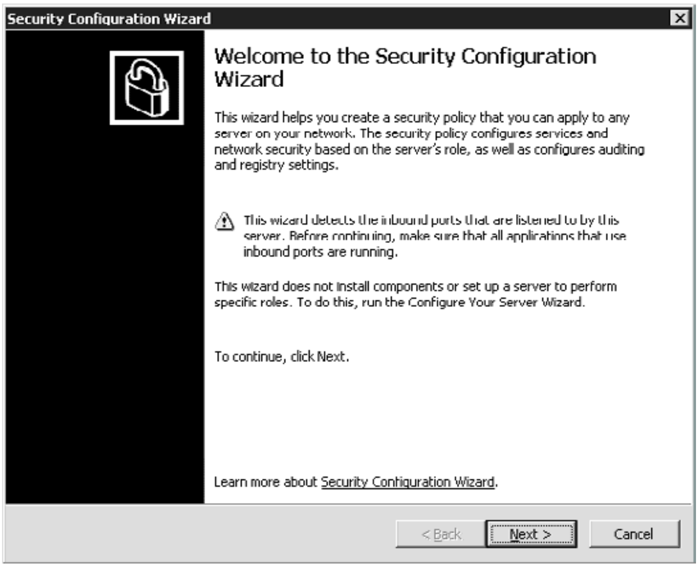
○ Off

Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

For information, see the Microsoft Web site.

Once the Firewall is running, run the Security Configuration Wizard as follows:

Start / Run / Scw
Or,
Start / Settings / Control Panel / Administrative Tools / 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.

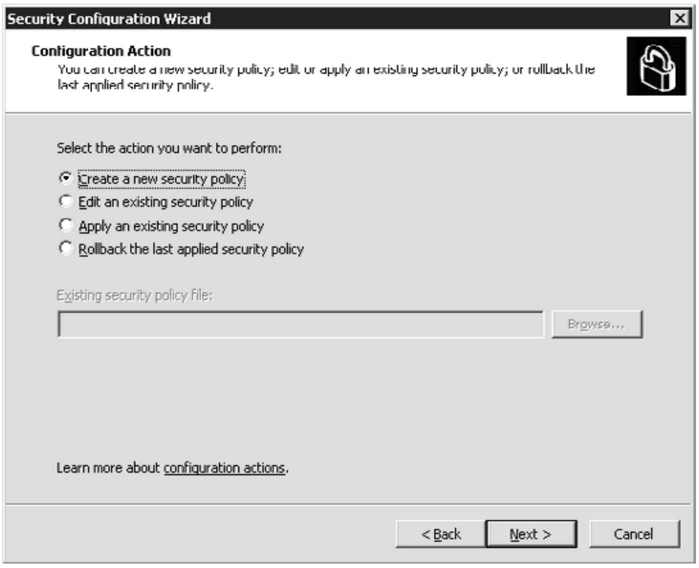
This wizard detects the inbound ports that are listened to by this server. Before continuing, make sure that all applications that use inbound ports are running.

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.

Select ‘Next’, then ‘Next’ again to create a new security policy



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.

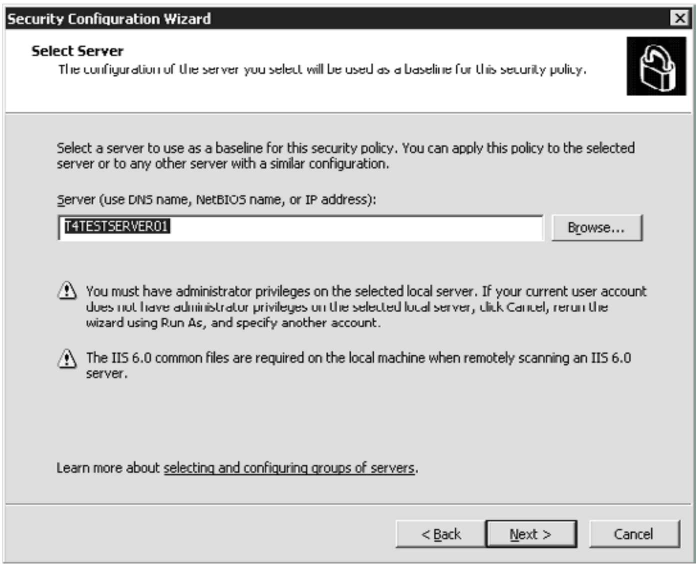
Select the action you want to perform:

● 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.

Confirm that the hostname is that of the PC being configured, then select ‘Next’:



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): T4TESTSERVER01

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.

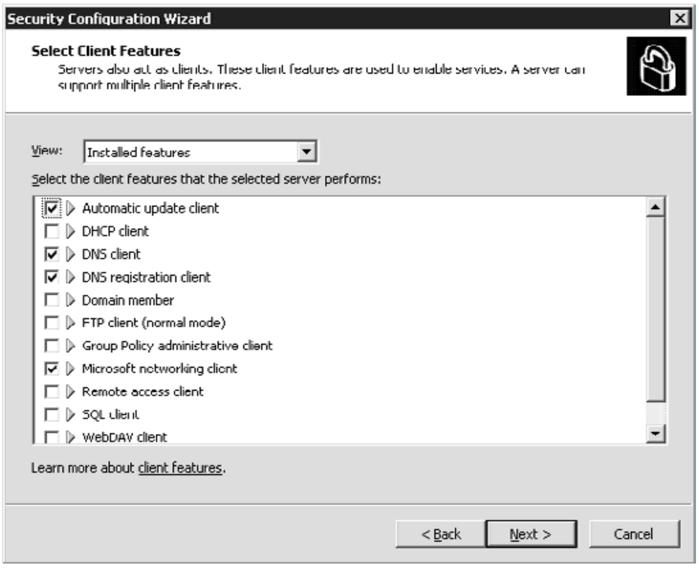
Database configuration will then process – select ‘Next’ when complete.
At Role Based Configuration – select ‘Next’.

Select Server Roles
NOTE – Important items to leave checked for CCC are:

- Application Sever (IIS to be pre-installed)
- ASP.Net Session state server (if missing cancel out and add asp.net found under Settings / Control Panel / Add/Remove Programs / Add/Remove Windows Components / Application Server / details)
- Middle Tier Application Server

- SQLServer2000 – which also covers MSDE
- Web Server

Confirm that the installed features are correct – otherwise accept defaults, select ‘Next’ to configure:



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.

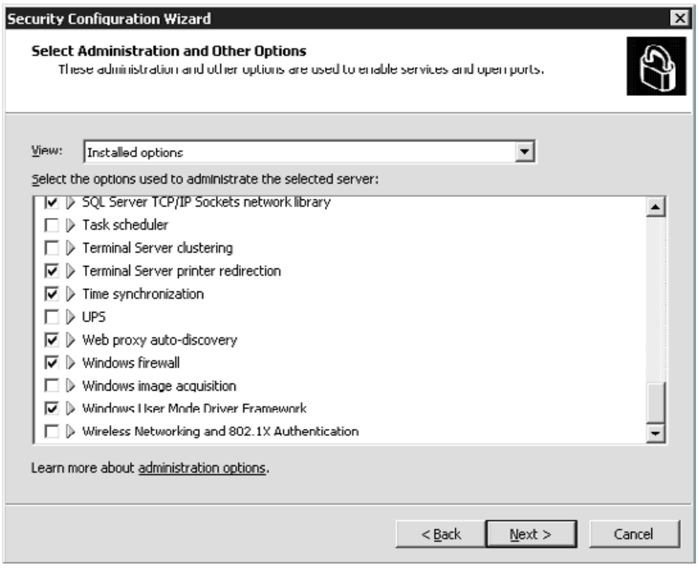
View: Installed features

Select the client features that the selected server performs:

- ☑ Automatic update client
- □ 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

Learn more about client features.

Installed Options – leave default, select ‘Next’ to continue.



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:

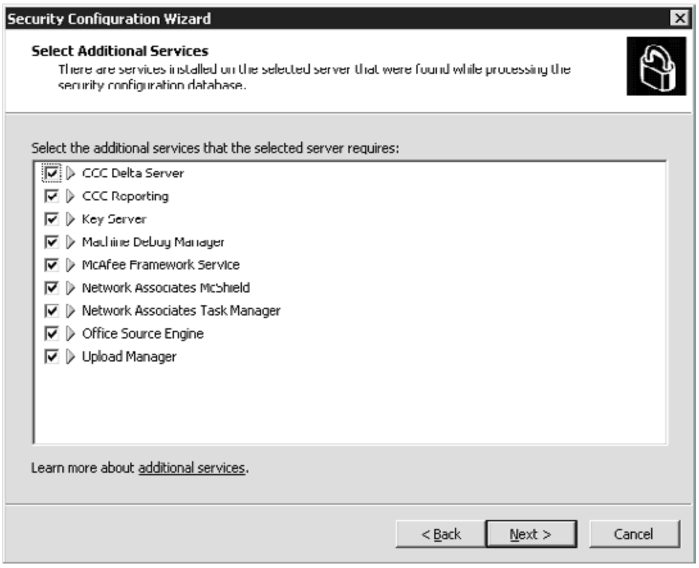
- ☑ SQL Server TCP/IP Sockets network library
- □ Task scheduler
- □ Terminal Server clustering
- ☑ Terminal Server printer redirection
- ☑ Time synchronization
- □ UPS
- ☑ Web proxy auto-discovery
- ☑ Windows firewall
- □ Windows image acquisition
- ☑ Windows User Mode Driver Framework
- □ Wireless Networking and 802.1X Authentication

Learn more about administration options.

Additional Services
NOTE – Key components for CCC are:

- CCC Delta Server
- CCC Reporting
- Key Server

Confirm that all the IP Office services are ticked, then select ‘Next’ to continue:



Select Additional Services

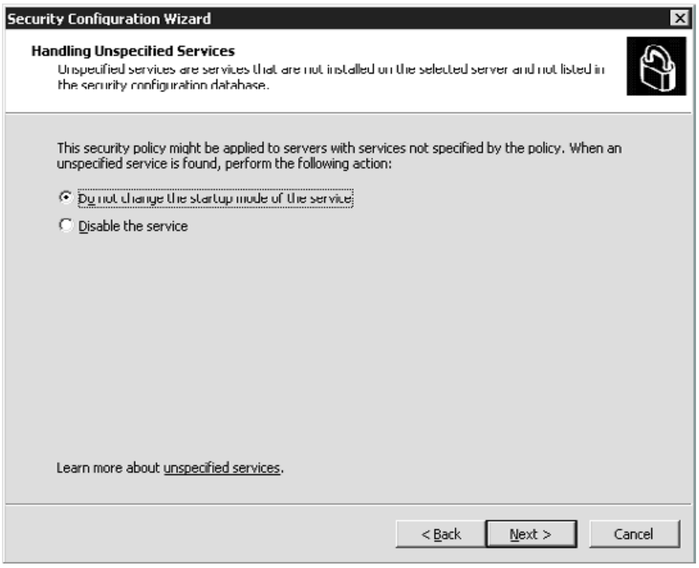
There are services installed on the selected server that were found while processing the security configuration database.

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

Learn more about additional services.

Unspecified Services – select ‘Do not change…’ then select ‘Next’ to continue:



Handling Unspecified Services

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

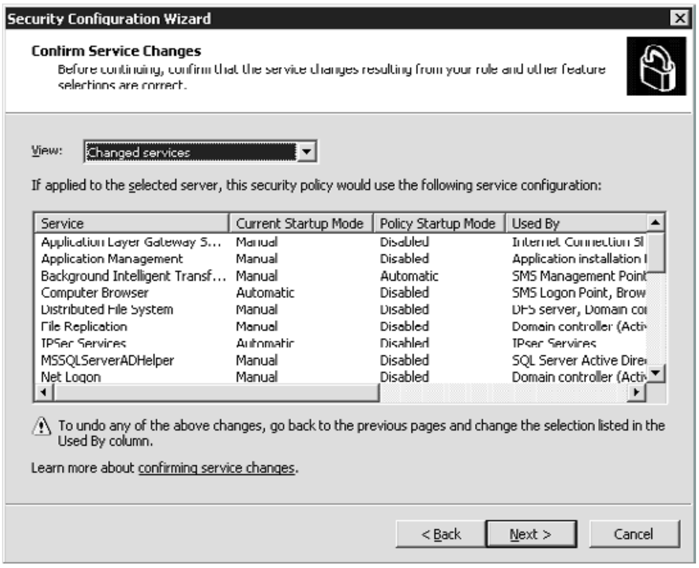
This security policy might be applied to servers with services not specified by the policy. When an unspecified service is found, perform the following action:

● Do not change the startup mode of the service

○ Disable the service

Learn more about unspecified services.

Review the changed Services and confirm that any changes have been applied:



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 Sl
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.

At the Network Security dialog, select ‘Next’ to continue.

At the Open Ports and Approve Applications dialog, note the CCC items when scrolling through list, and confirm that they have been selected.

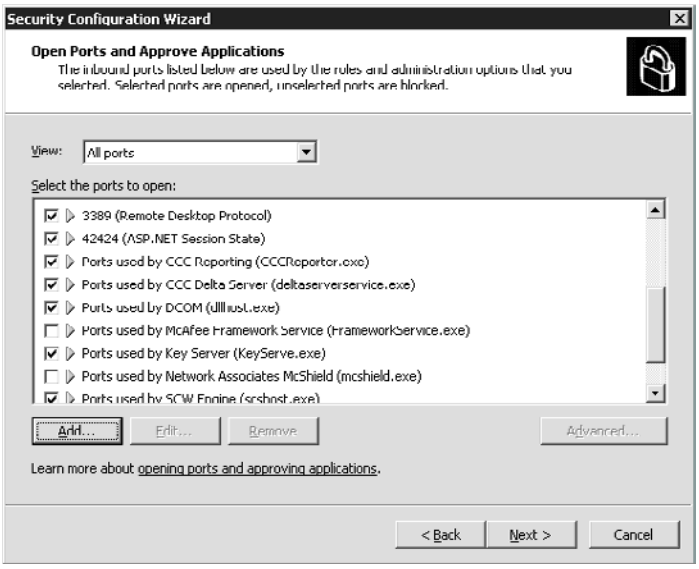
NOTE – Optional Step - ADD PC Wallboard Server application at this time. Otherwise you will have the option of setting a program exclusion for Windows Firewall when the Wallboard Server is first started.

To add – Click “Add” / Approve Application / Browse for PC Wallboard Server (default location is: C:\Program Files\AVAYA\IP Office\CCC\WBServer\wbserver32.exe)

You will see Ports used by wbserver.exe added to the approved application list

☑ Ports used by wbserver32.exe

Confirm that all CCC and IP Office applications have an entry in the Port Confirmation dialog, then select ‘Next’ to continue.



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

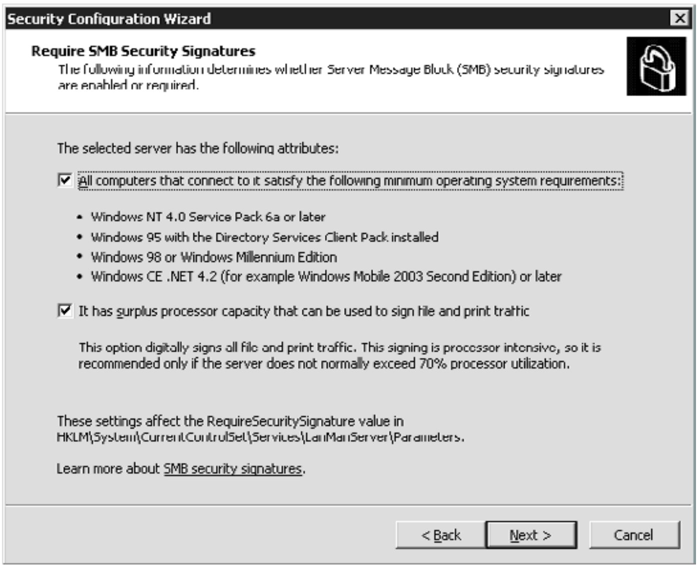
Select the ports to open:

- ☑ 3389 (Remote Desktop Protocol)
- ☑ 42424 (ASP.NET Session State)
- ☑ Ports used by CCC Reporting (CCCReporter.exe)
- ☑ Ports used by CCC Delta Server (deltaserverservice.exe)
- ☑ 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)

Learn more about opening ports and approving applications.

Accept the defaults for the Registry Settings dialog, then select ‘Next’ to continue.

Accept the defaults for the Require SMB Security Signatures dialog, then select ‘Next’ to continue:



Security Configuration Wizard

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

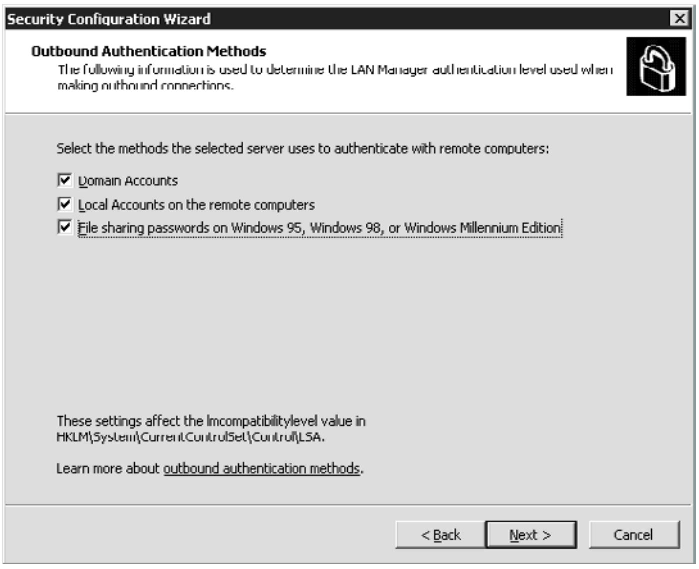
☑ It has surplus processor capacity that can be used to sign file and print traffic

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.

At the Outbound Authentication Methods dialog, select the options required for the system depending upon the Operating systems in use on the system, and whether or not remote access is required.   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

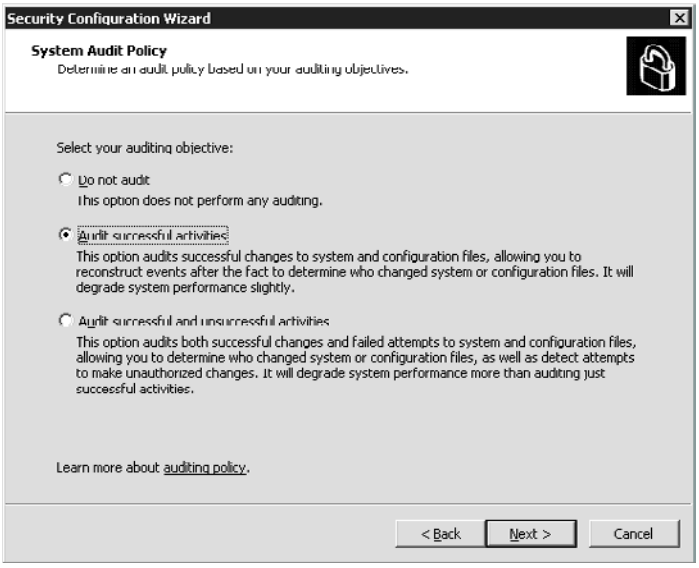
☑ File sharing passwords on Windows 95, Windows 98, or Windows Millennium Edition

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

Learn more about outbound authentication methods.

Verify that the settings chosen at the settings summary are correct, then select ‘Next’ to continue.

At the System Audit Policy screen, the options can be set as desired or leave default. Select ‘Next’ to continue.



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.

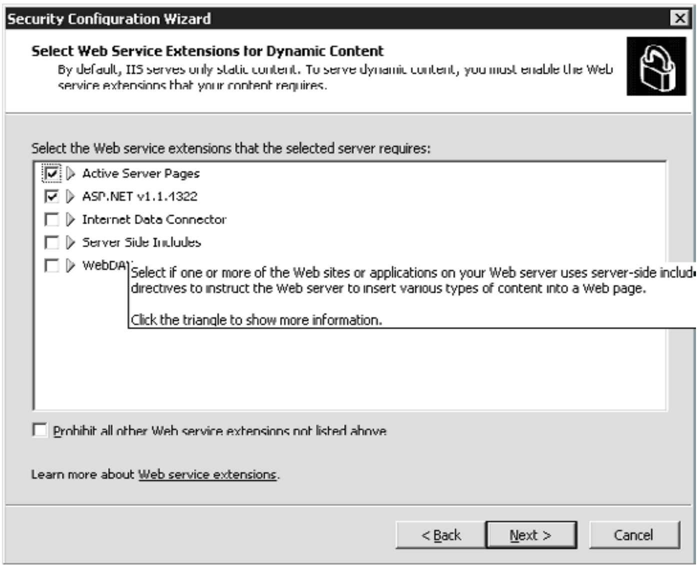
○ Audit successful and unsuccessful activities
This option audits both successful changes and failed attempts to system and configuration files, allowing you to determine who changed system or configuration files, as well as detect attempts to make unauthorized changes. It will degrade system performance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

Learn more about auditing policy.

Verify summary then select ’Next’ to continue.

At the Internet Information Services screen, select ‘Next’ to continue.

Select Active Server pages and ASP.Net then select ‘Next’ to continue:



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
- ☑ ASP.NET v1.1.4322
- ☐ Internet Data Connector
- ☐ Server Side Includes
- ☐ WebDA

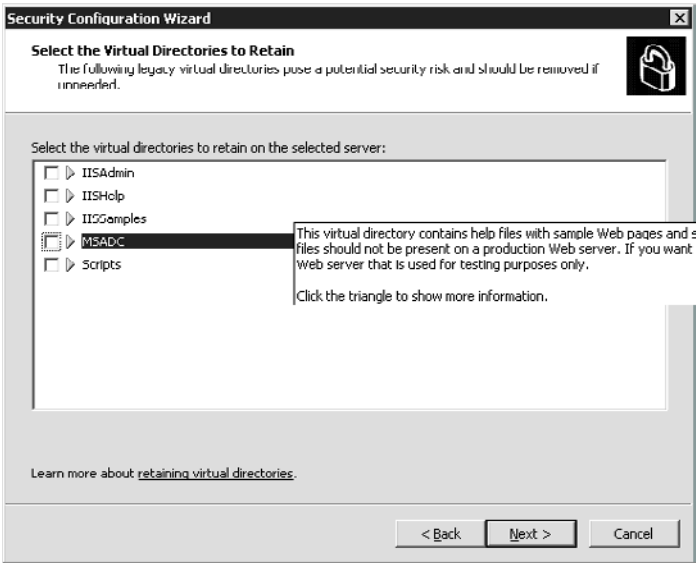
Select if one or more of the Web sites or applications on your Web server uses server-side includ directives to instruct the Web server to insert various types of content into a Web page.

Click the triangle to show more information.

☐ Prohibit all other Web service extensions not listed above

Learn more about Web service extensions.

Confirm the defaults at the Virtual Directories to retain screen by selecting ‘Next’ to continue:



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:

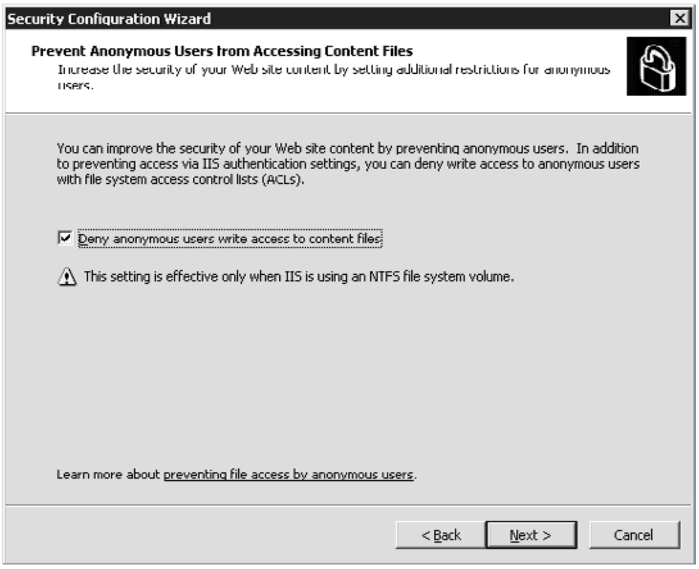
- ☐ IISAdmin
- ☐ IISHelp
- ☐ IISSamples
- ☐ MSADC
- ☐ Scripts

This virtual directory contains help files with sample Web pages and s files should not be present on a production Web server. If you want Web server that is used for testing purposes only.

Click the triangle to show more information.

Learn more about retaining virtual directories.

Prevent Anonymous Users from Accessing Content Files - Check to DENY anonymous access, then 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).

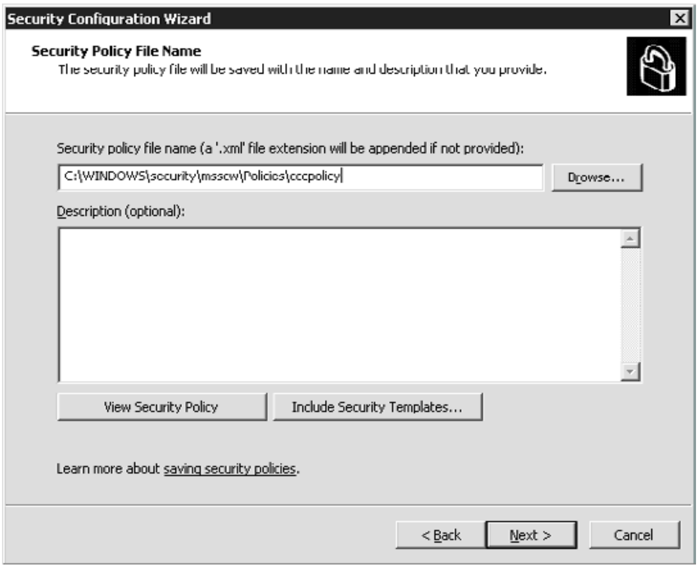
☑ Deny anonymous users write access to content files

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

Learn more about preventing file access by anonymous users.

Review the IIS settings summary page, then select ‘Next’ to continue.

At the Save Security Policy dialog, provide a filename and location – for example cccpolicy, then select ‘Next’ to continue:



Security Configuration Wizard

Security Policy File Name

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

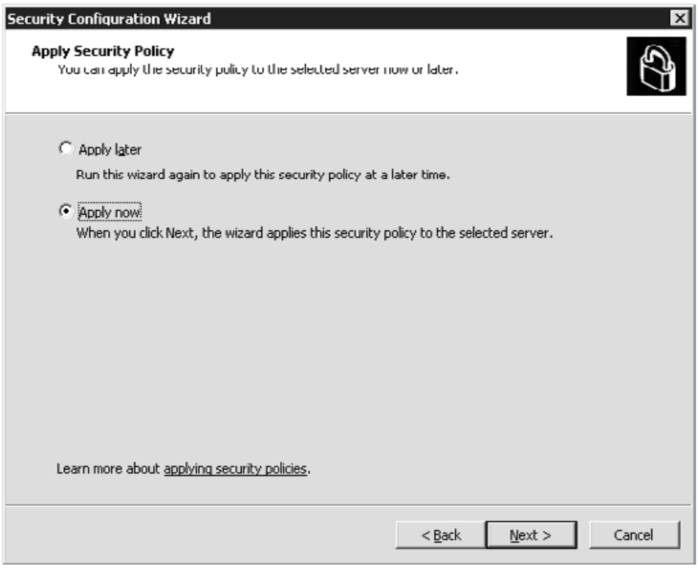
Security policy file name (a '.xml' file extension will be appended if not provided):

C:\WINDOWS\security\msscw\Policies\cccpolicy

Description (optional):

Learn more about saving security policies.

Select ‘Apply Now’ then ‘Next’ to confirm:



Apply Security Policy

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

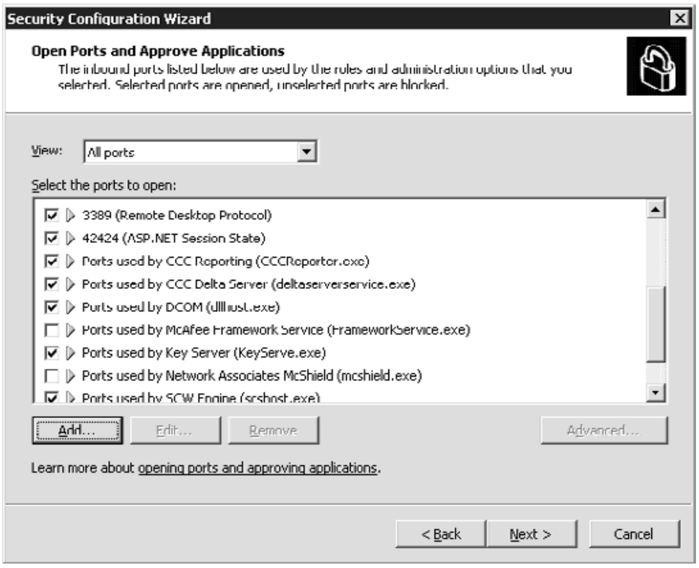
○ Apply later

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.



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.

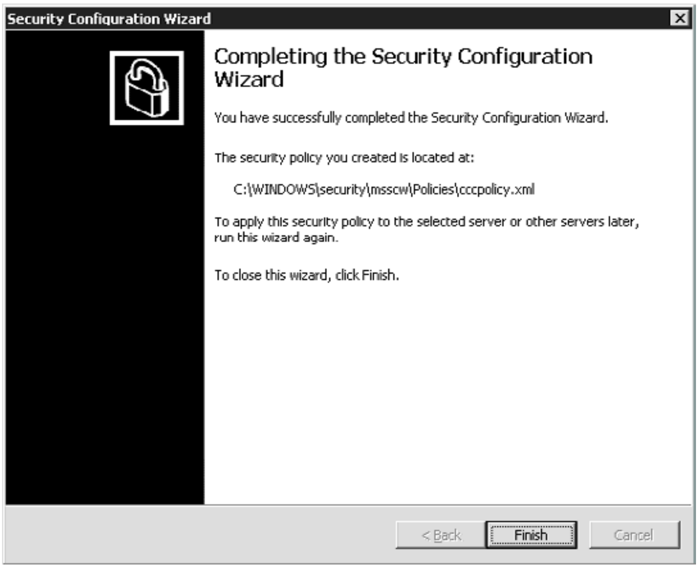
View: All ports

Select the ports to open:

- ☑ 3389 (Remote Desktop Protocol)
- ☑ 42424 (ASP.NET Session State)
- ☑ Ports used by CCC Reporting (CCCReporter.exe)
- ☑ Ports used by CCC Delta Server (deltaserverservice.exe)
- ☑ 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)

Learn more about opening ports and approving applications.

The Security Configuration Wizard will then process and apply the configuration.



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\cccpolicy.xml

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

To close this wizard, click Finish.

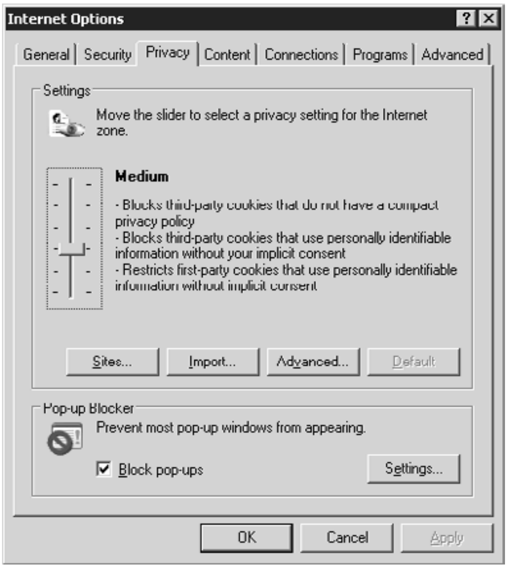
On completion of the Security Configuration Wizard, select ‘Finish’, then reboot the server for the changes to fully take effect.

Enable CCC Reporting website “pop-up”

CCC Reporter is seen as an Application pop-up in Internet Explorer so has to added to the exclude list under the Internet Explorer Privacy settings

Select Tools / Internet options / Privacy / Pop-up Blocker section / Settings

Then enter http://<server hostname>/Reporting and add to “allowed sites”.



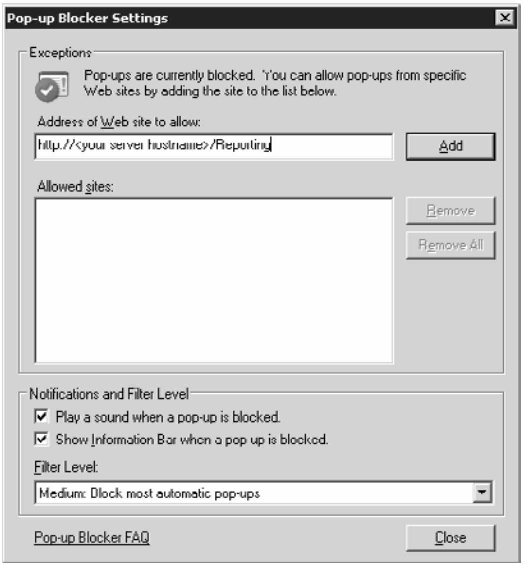
Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Prevent most pop-up windows from appearing.

☑ Block pop-ups



Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.

Address of Web site to allow: http://<your server hostname>/Reporting

Allowed sites:

Notifications and Filter Level

☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop up is blocked.

Filter Level: Medium: Block most automatic pop-ups

NOTE – even if the full URL is used it will resolve the hostname of your CCC Server

Select ‘Ok’ then ‘Close’ and ‘Ok’ to finish.
CCC Reporting will now allow the “pop-up” application window.

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