



## 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>

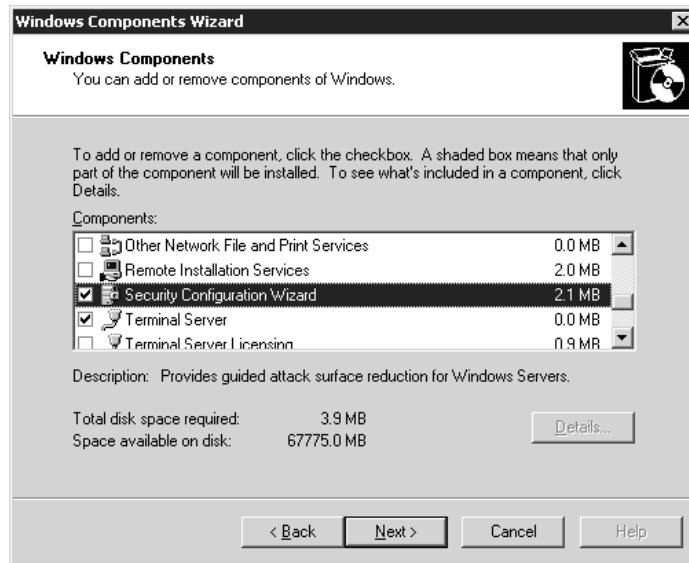
The security policy enforced by SP1 requires modifications in order for the IP Office Compact Contact Center (CCC) suite of client/server applications to work properly and maintain functionality. This document will cover the post Windows Server 2003 Service Pack 1 modifications needed for IP Office CCC.

#### **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':



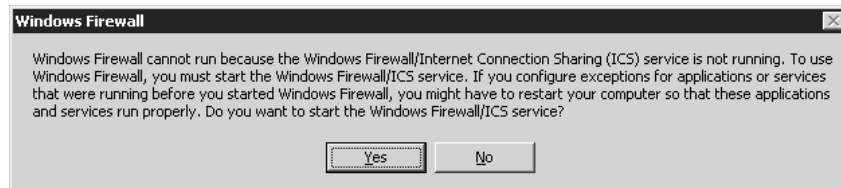
Click 'Finish' when complete.

### **Initialize Firewall**

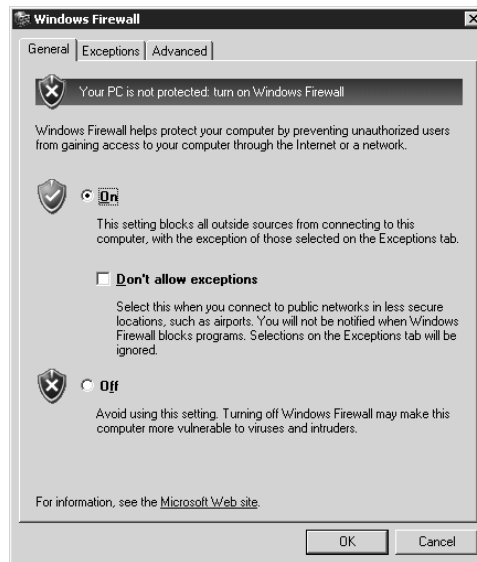
Once the Security Configuration Wizard has run, Windows Firewall needs to be started:

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

The following confirmation prompt is displayed:



Select 'Yes' to turn the Firewall on:



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

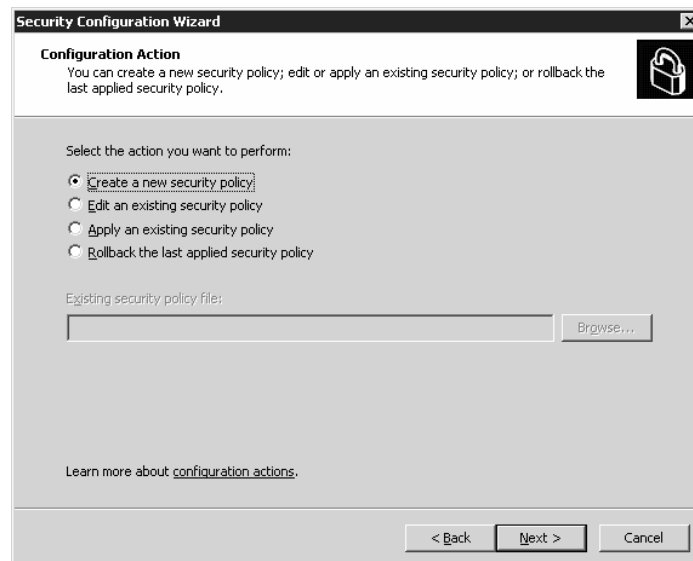
Start / Run / Scw

Or,

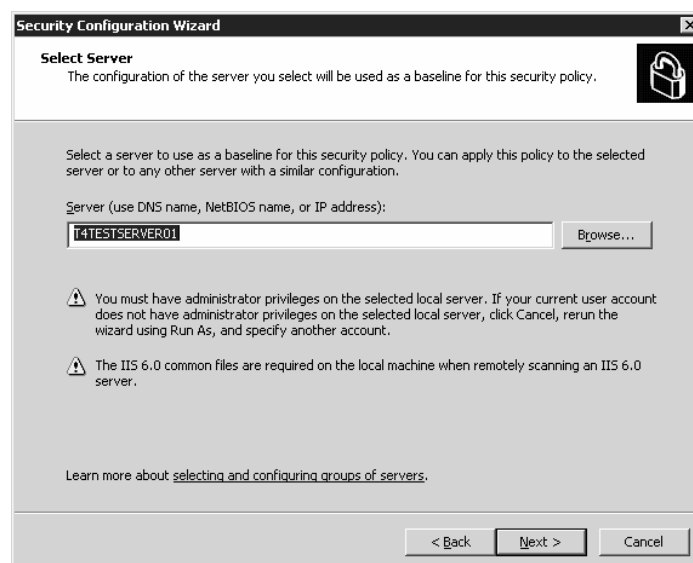
Start / Settings / Control Panel / Administrative Tools / Security Configuration Wizard:



Select 'Next', then 'Next' again to create a new security policy



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



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

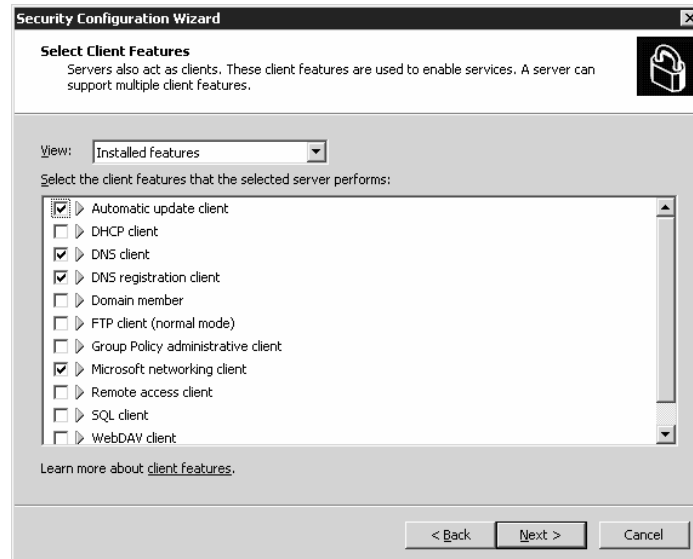
#### Select Server Roles

NOTE – Important items to leave checked for CCC are:

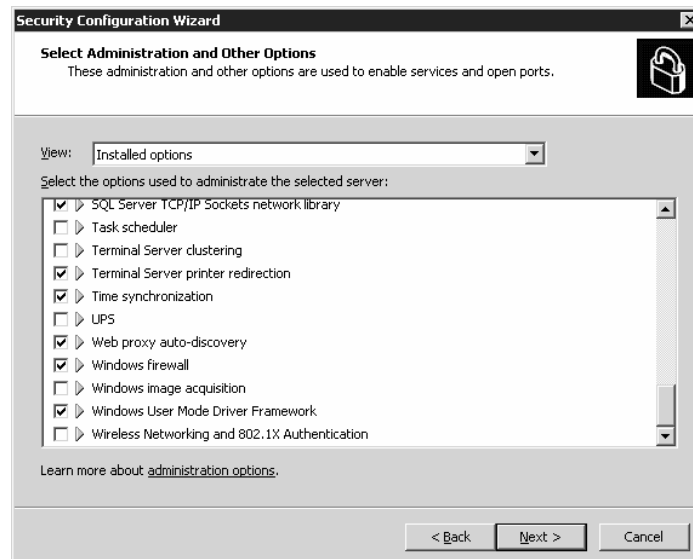
- Application Server (IIS to be pre-installed)
- ASP.Net Session state server (if missing cancel out and add asp.net found under Settings / Control Panel / Add/Remove Programs / Add/Remove Windows Components / Application Server / details)
- Middle Tier Application Server

- SQLServer2000 – which also covers MSDE
- Web Server

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



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

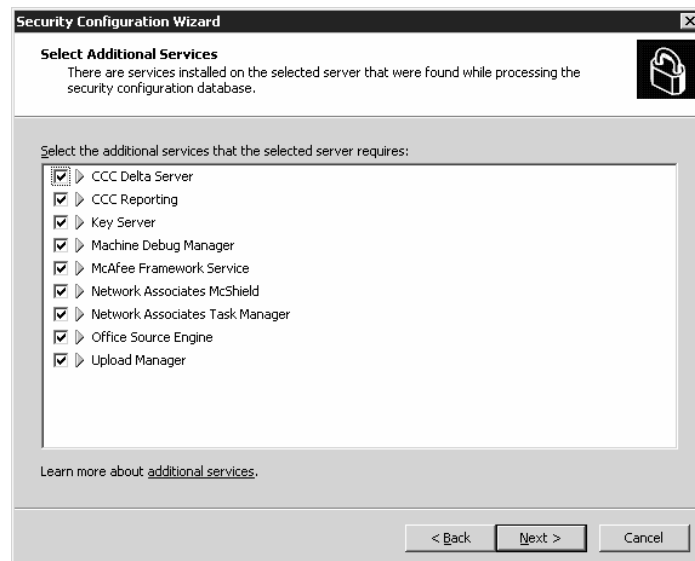


#### Additional Services

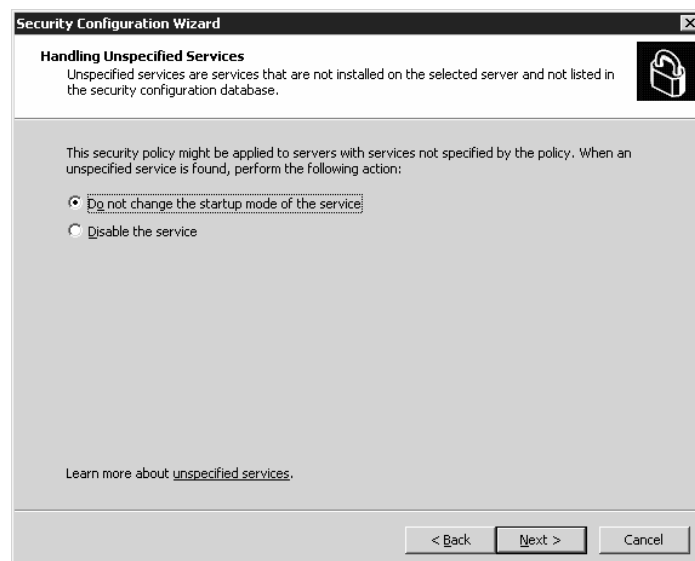
NOTE – Key components for CCC are:

- CCC Delta Server
- CCC Reporting
- Key Server

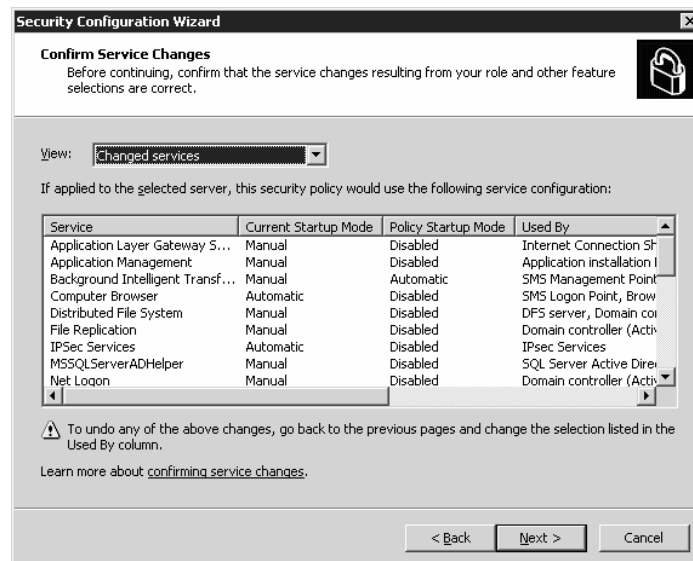
Confirm that all the IP Office services are ticked, then select 'Next' to continue:



Unspecified Services – select 'Do not change...' then select 'Next' to continue:



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



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.

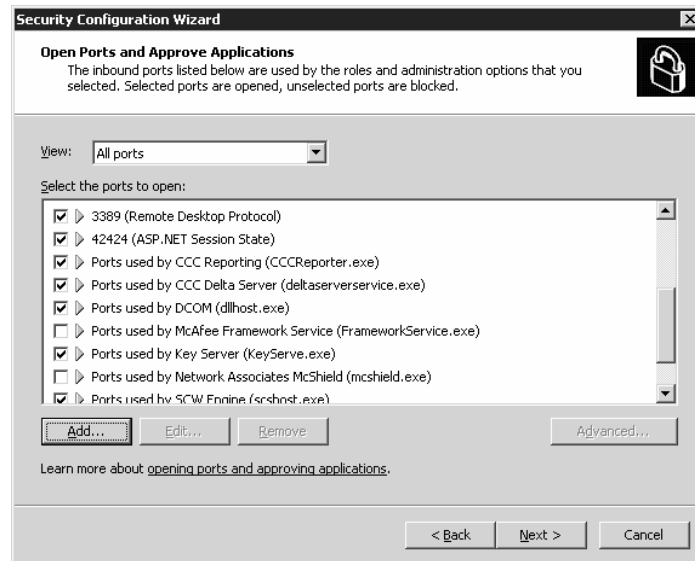
NOTE – Optional Step - ADD PC Wallboard Server application at this time. Otherwise you will have the option of setting a program exclusion for Windows Firewall when the Wallboard Server is first started.

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



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



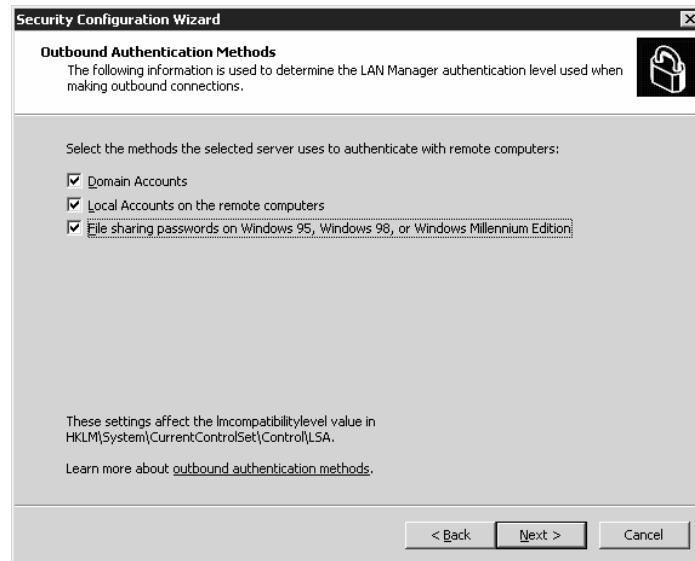
Accept the defaults for the Registry Settings dialog, then select 'Next' to continue.

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



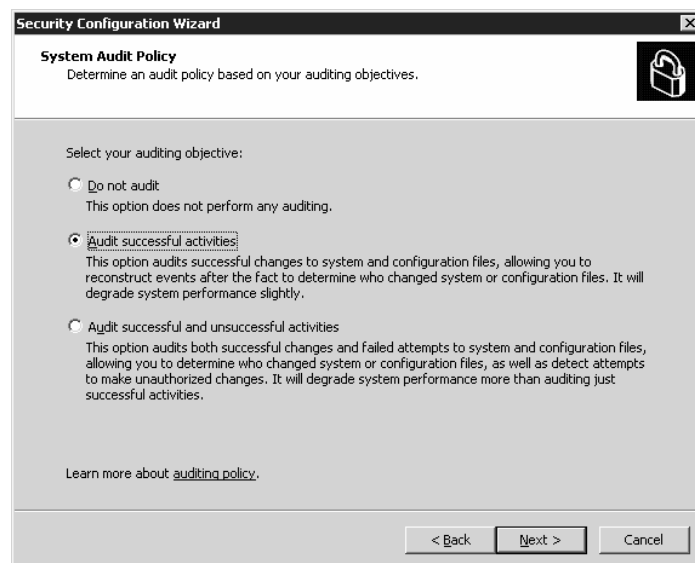
At the Outbound Authentication Methods dialog, select the options required for the system depending upon the Operating systems in use on the system, and whether or not remote access is required. Select 'Next' to continue.





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

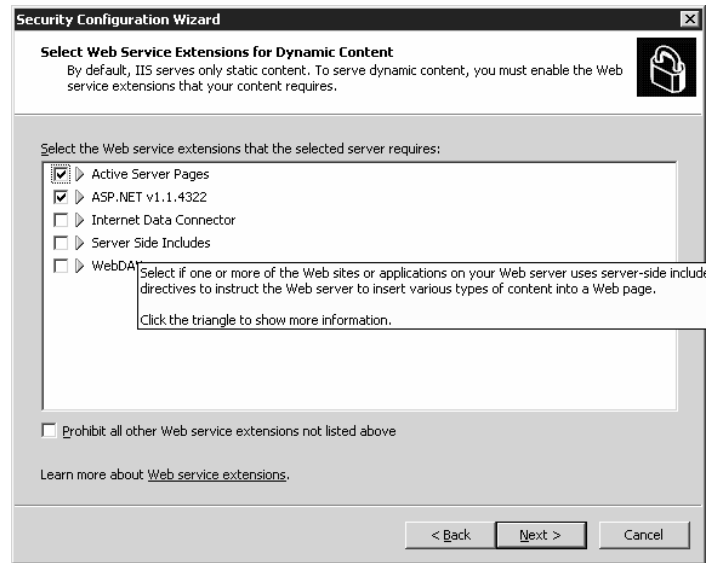
At the System Audit Policy screen, the options can be set as desired or leave default. Select 'Next' to continue.



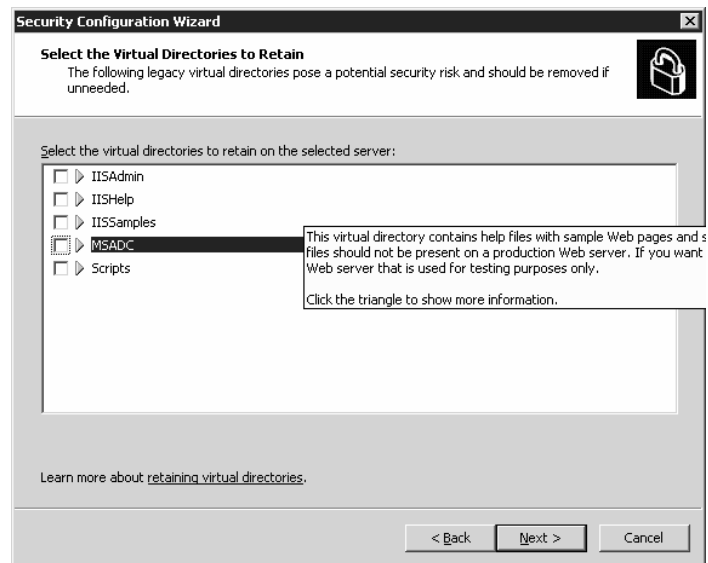
Verify summary then select 'Next' to continue.

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

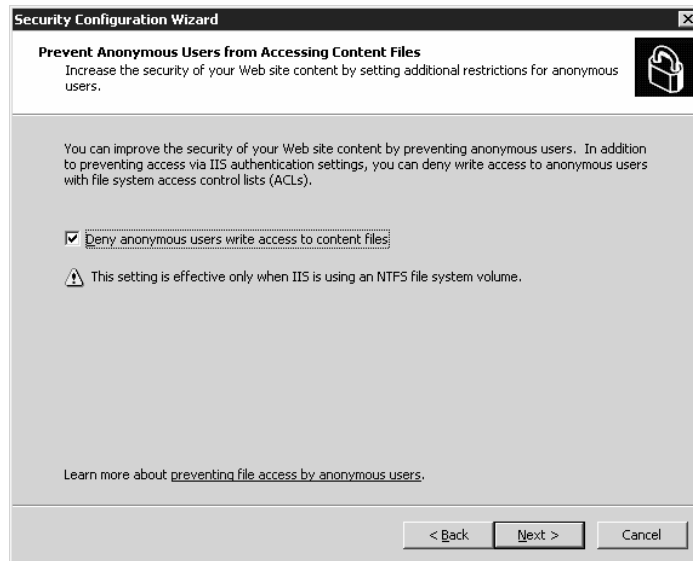
Select Active Server pages and ASP.Net then select 'Next' to continue:



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

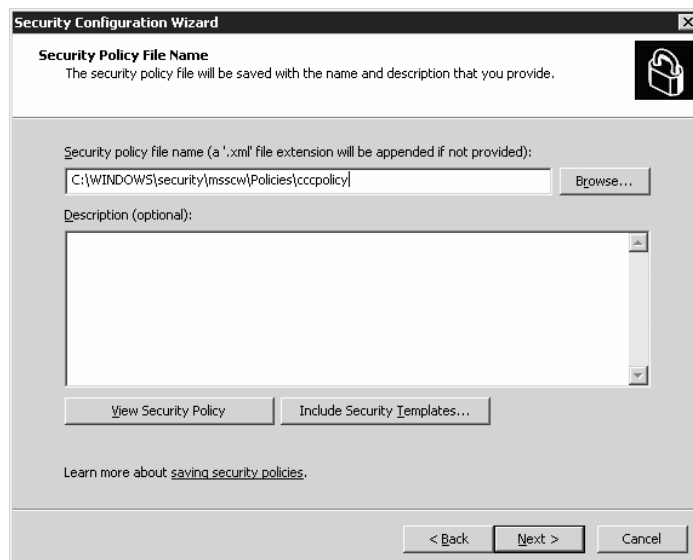


Prevent Anonymous Users from Accessing Content Files - Check to DENY anonymous access, then select 'Next' to continue:

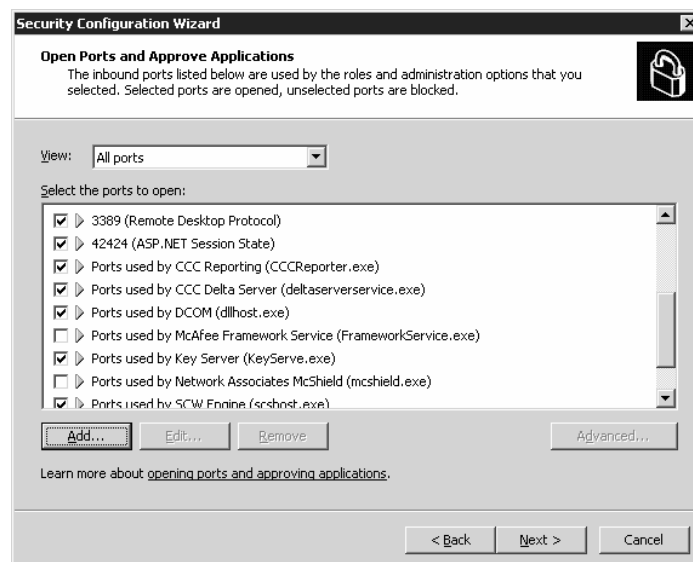


Review the IIS settings summary page, then select 'Next' to continue.

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



Select 'Apply Now' then 'Next' to confirm:



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



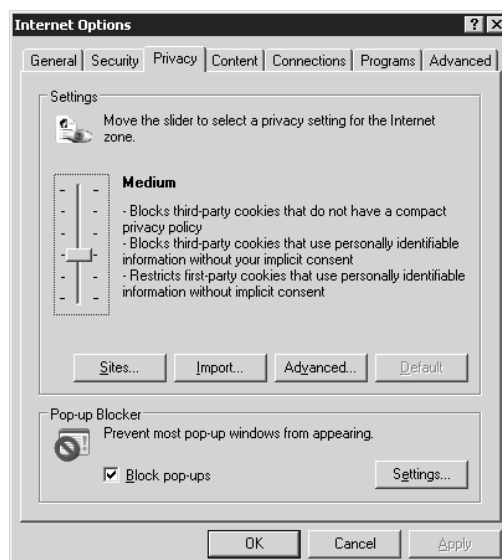
On completion of the Security Configuration Wizard, select 'Finish', then reboot the server for the changes to fully take effect.

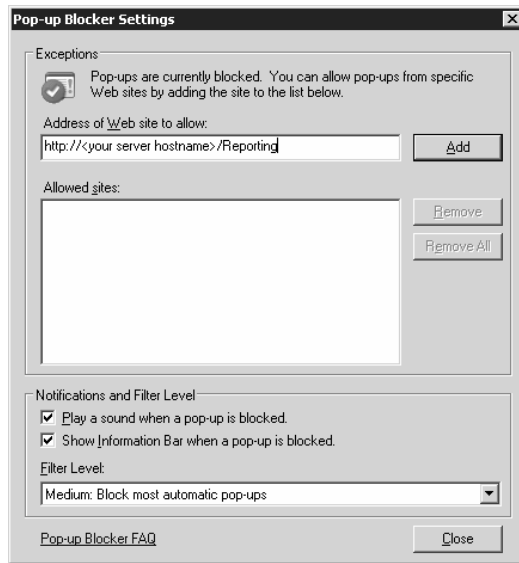
### **Enable CCC Reporting website “pop-up”**

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”.





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](mailto:gsstier4@avaya.com)*

*NA/CALA*  
*Tel: +1 732 852 1955*  
*Fax: +1 732 852 1943*  
*Email: [IPOUST4ENG@Avaya.com](mailto:IPOUST4ENG@Avaya.com)*

*Internet: <http://www.avaya.com>*  
© 2006 Avaya Inc. All rights reserved.