PUBLISHING A WINDOWS SERVER 2003 CERTIFICATION AUTHORITY WEB ENROLLMENT SITE AND CERTIFICATE REVOCATION LIST

There may be circumstances when you may wish to access the Web enrollment site from an external network client. This is most common when the external client needs to obtain an IPSec certificate from a standalone CA on your internal network. Machines don't typically need to access an enterprise CA because certificates are more easily obtained via certificate autoenrollment or the Certificates MMC snap-in.

Publishing the Certificate Web enrollment works like any other type of Web publishing. The specific procedures required to publish a Certificate Server Web enrollment site include:

- Install Internet Information Server and the Standalone Certification Authority
- Identify the Location of the CRL and configure the CRL publishing site and the AIA for the CTL (Certificate Trust List)
- Create a DNS entry in the public DNS
- Install ISA Server 2000 and configure the Incoming Web Requests listener
- Create the Destination Set and HOSTS file entry to support the Web Publishing Rule
- Create the Web Publishing Rule

We will cover each of these procedures in this **ISA Server 2000 VPN Deployment Kit** document.

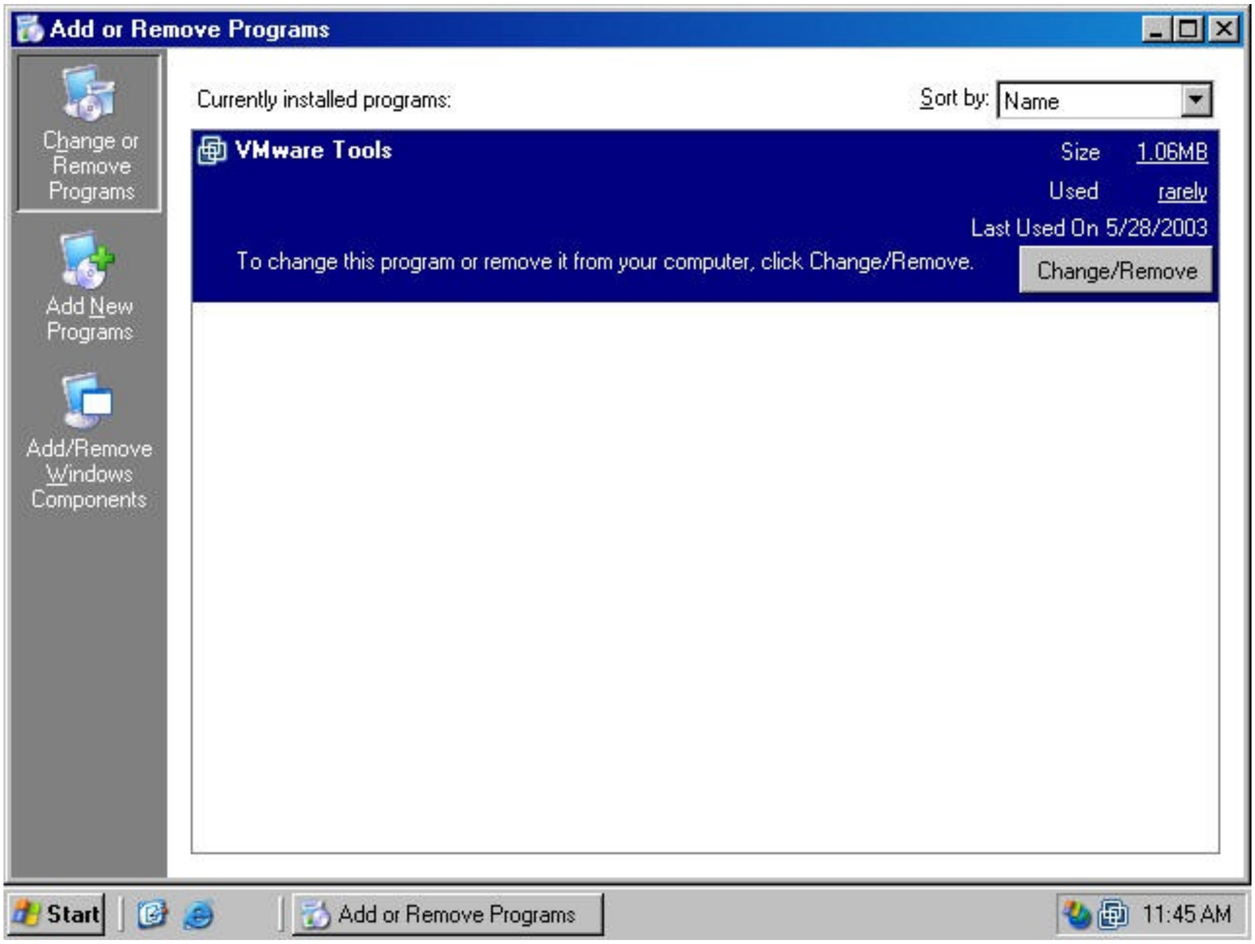
Install Internet Information Server (IIS) and the Standalone Certification Authority

The Web enrollment site requires the Internet Information Service World Wide Web service (W3SVC). You must install IIS before installing Microsoft Certificate Services. IIS is installed by default on Windows 2000, but it is not installed by default in Windows Server 2003.

Perform the following steps to install IIS 6.0 on the Windows Server 2003 member server or domain controller computer that act as a standalone CA:

1. Click **Start**, point to **Control Panel** and click **Add or Remove Programs**.
2. Click the **Add/Remove Windows Components** button in the **Add or Remove Programs** window (figure 1).

Figure 1



Currently installed programs:

Sort by: Name

VMware Tools

Size 1.06MB

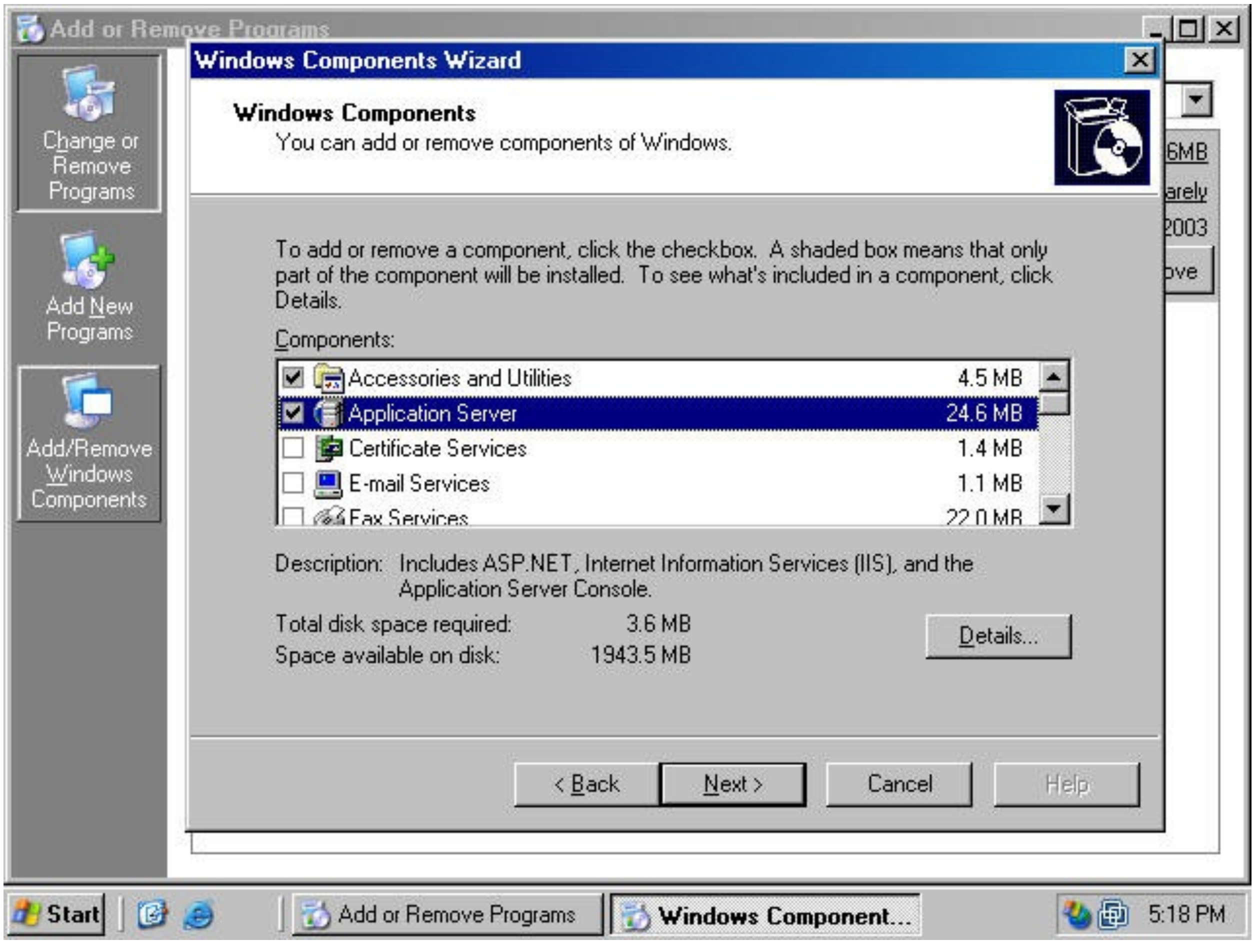
Used rarely

Last Used On 5/28/2003

To change this program or remove it from your computer, click Change/Remove.

3. On the **Windows Components** window, click on the **Application Server** entry and click the **Details** button (figure 2).

Figure 2



Windows Components Wizard

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:

☑ Accessories and Utilities	4.5 MB
☑ Application Server	24.6 MB
□ Certificate Services	1.4 MB
□ E-mail Services	1.1 MB
□ Fax Services	22.0 MB

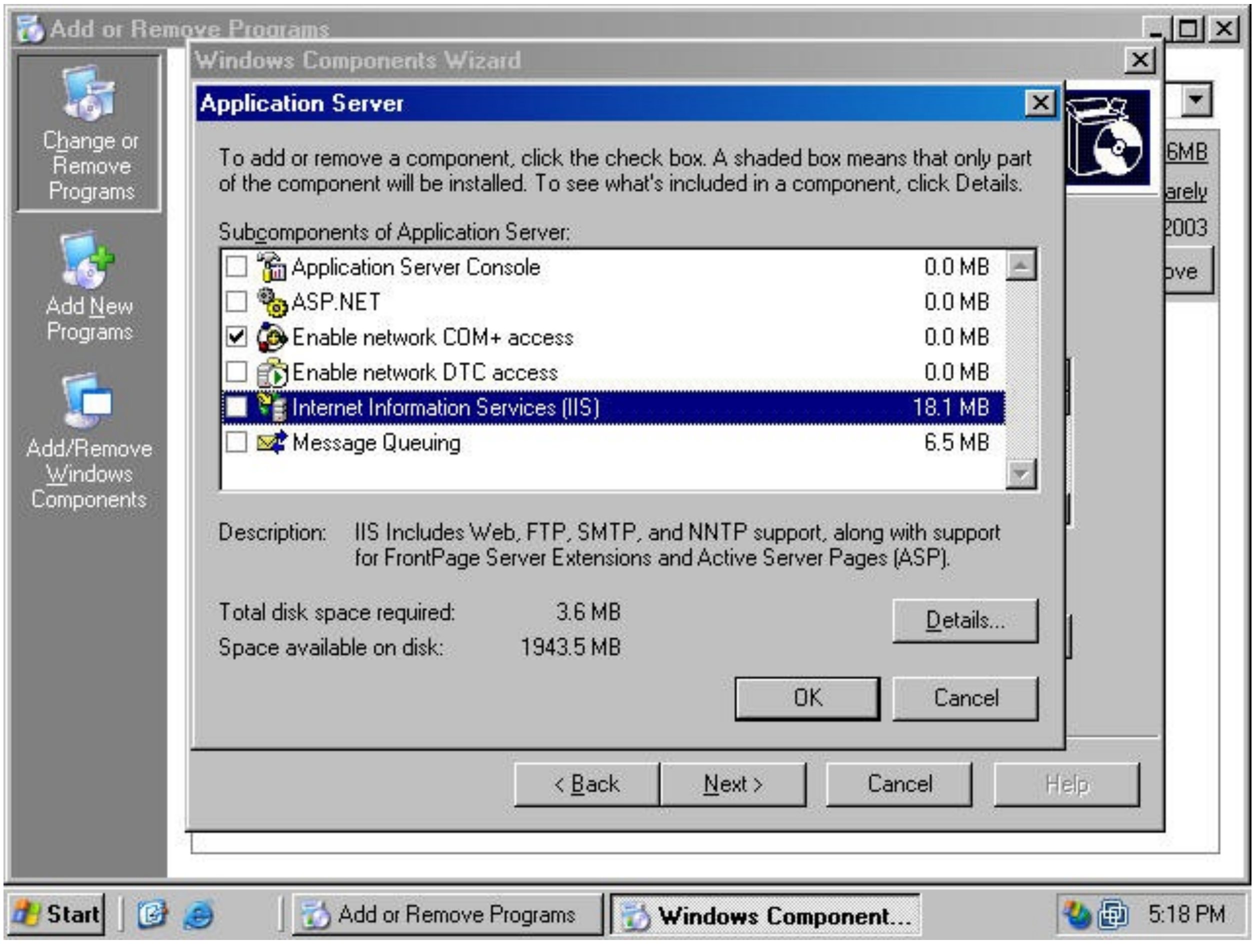
Description: Includes ASP.NET, Internet Information Services (IIS), and the Application Server Console.

Total disk space required: 3.6 MB

Space available on disk: 1943.5 MB

4. On the **Application Server** page (figure 3), click on the **Internet Information Services (IIS)** entry and click the **Details** button.

Figure 3



Application Server

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

Subcomponents of Application Server:

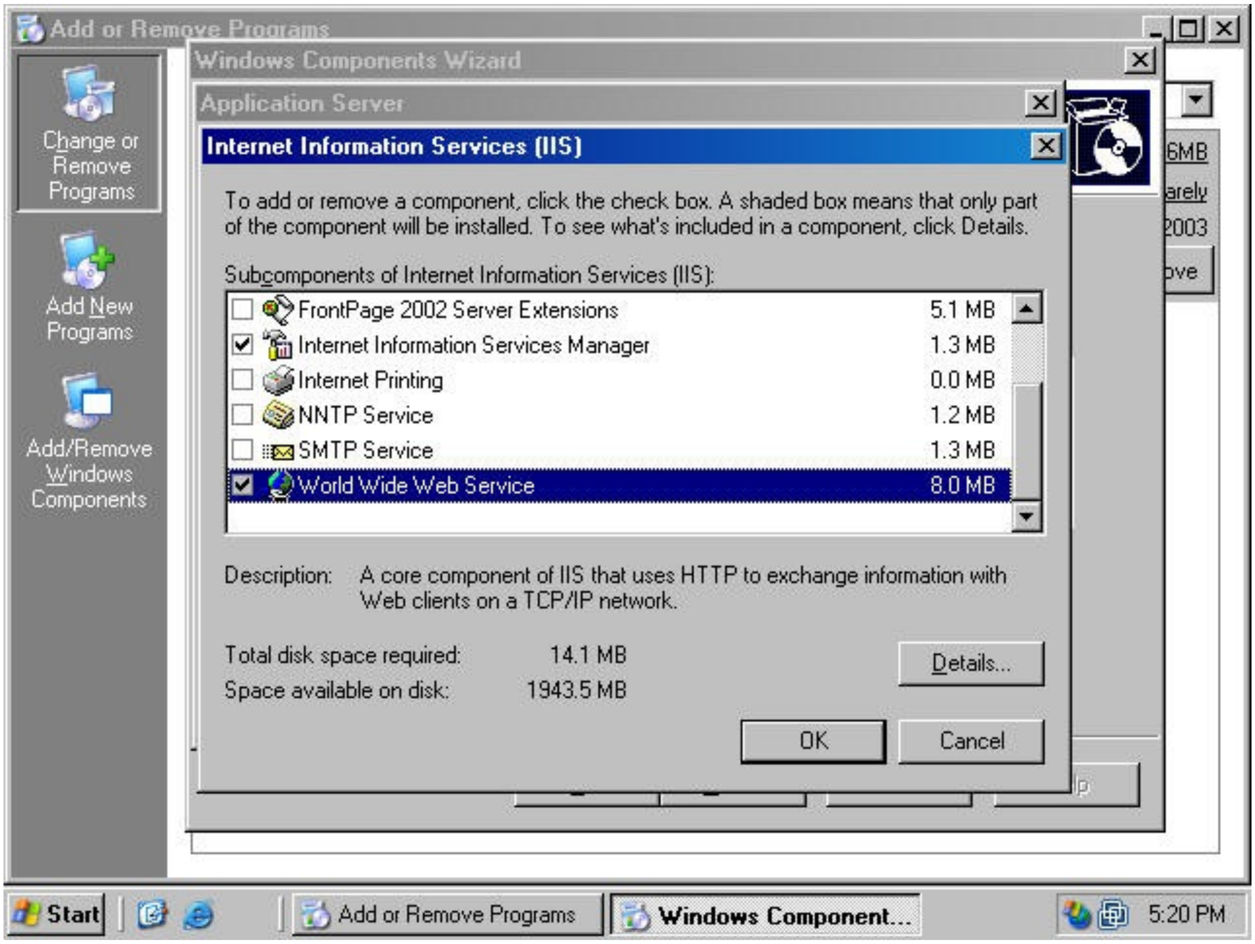
☐	Application Server Console	0.0 MB
☐	ASP.NET	0.0 MB
☑	Enable network COM+ access	0.0 MB
☐	Enable network DTC access	0.0 MB
☐	Internet Information Services (IIS)	18.1 MB
☐	Message Queuing	6.5 MB

Description: IIS Includes Web, FTP, SMTP, and NNTP support, along with support for FrontPage Server Extensions and Active Server Pages (ASP).

Total disk space required: 3.6 MB
Space available on disk: 1943.5 MB

5. In the **Internet Information Service (IIS)** dialog box (figure 4), put a checkmark in the **World Wide Web Service** checkbox and click **OK**.

Figure 4



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

Subcomponents of Internet Information Services (IIS):

☐	FrontPage 2002 Server Extensions	5.1 MB
☑	Internet Information Services Manager	1.3 MB
☐	Internet Printing	0.0 MB
☐	NNTP Service	1.2 MB
☐	SMTP Service	1.3 MB
☑	World Wide Web Service	8.0 MB

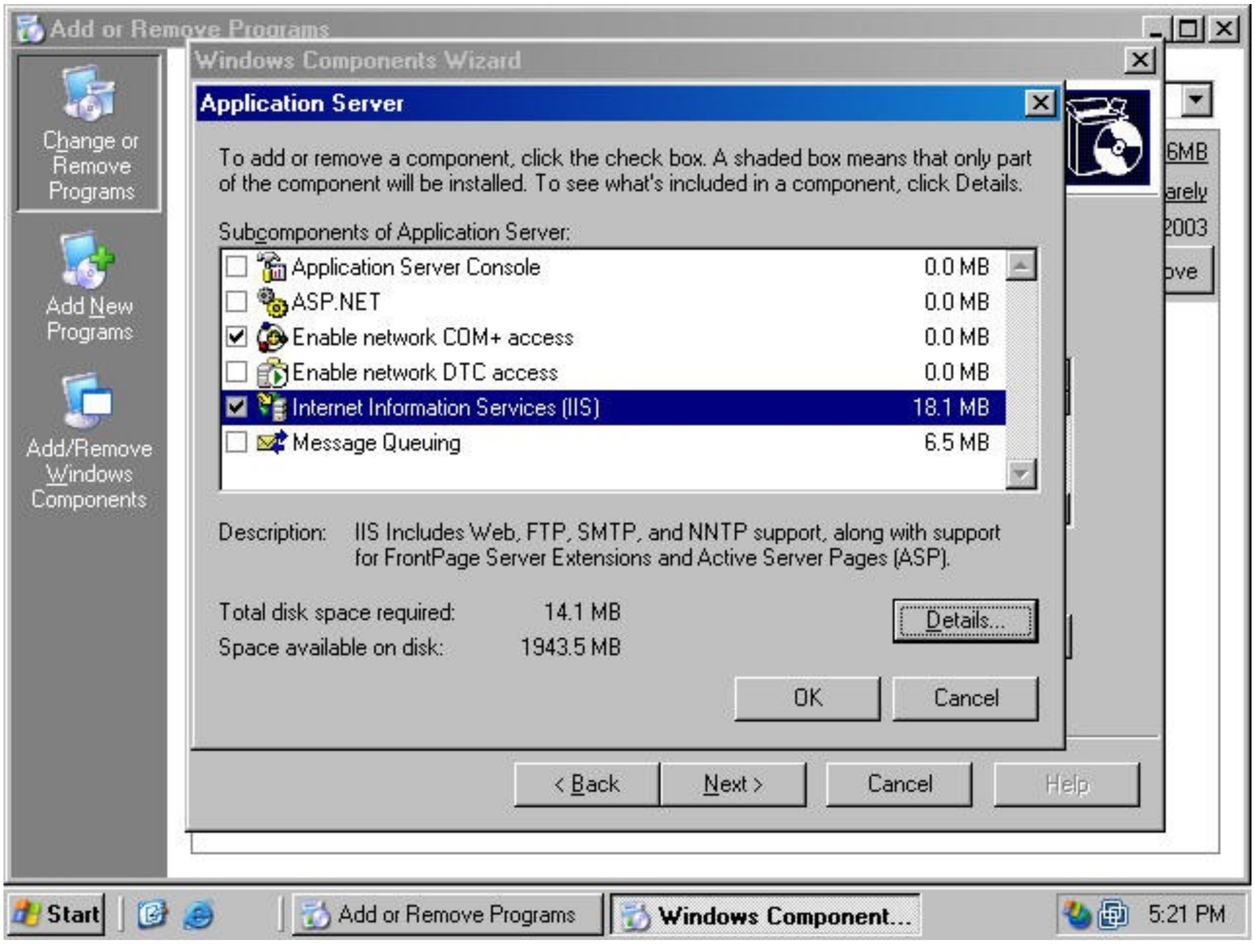
Description: A core component of IIS that uses HTTP to exchange information with Web clients on a TCP/IP network.

Total disk space required: 14.1 MB

Space available on disk: 1943.5 MB

6. Click **OK** on the **Application Server** dialog box (figure 5).

Figure 5



Application Server

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

Subcomponents of Application Server:

☐	Application Server Console	0.0 MB
☐	ASP.NET	0.0 MB
☑	Enable network COM+ access	0.0 MB
☐	Enable network DTC access	0.0 MB
☑	Internet Information Services (IIS)	18.1 MB
☐	Message Queuing	6.5 MB

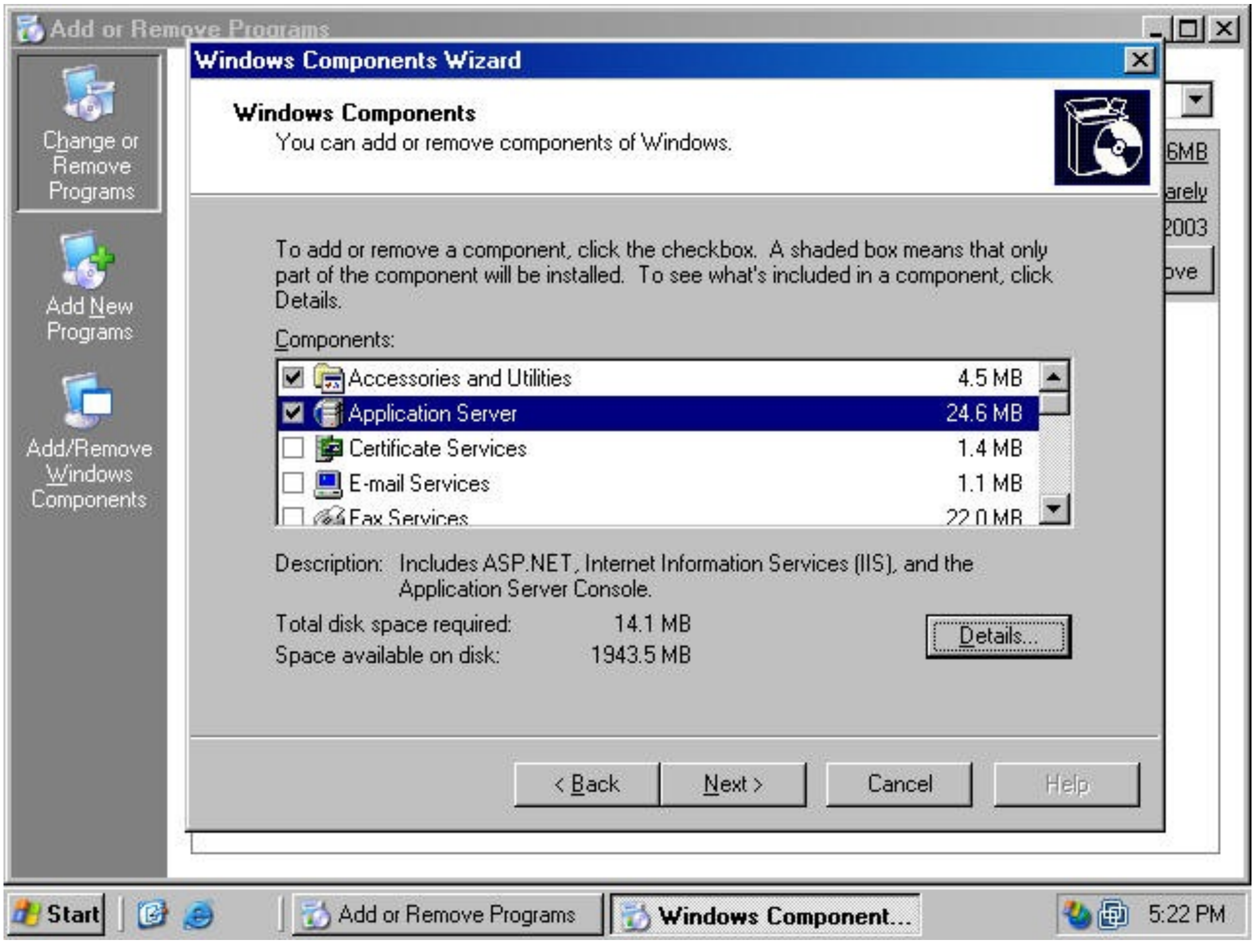
Description: IIS Includes Web, FTP, SMTP, and NNTP support, along with support for FrontPage Server Extensions and Active Server Pages (ASP).

Total disk space required: 14.1 MB

Space available on disk: 1943.5 MB

7. Click **Next** on the **Windows Components** dialog box (figure 6).

Figure 6



Windows Components Wizard

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:

☑	Accessories and Utilities	4.5 MB
☑	Application Server	24.6 MB
□	Certificate Services	1.4 MB
□	E-mail Services	1.1 MB
□	Fax Services	22.0 MB

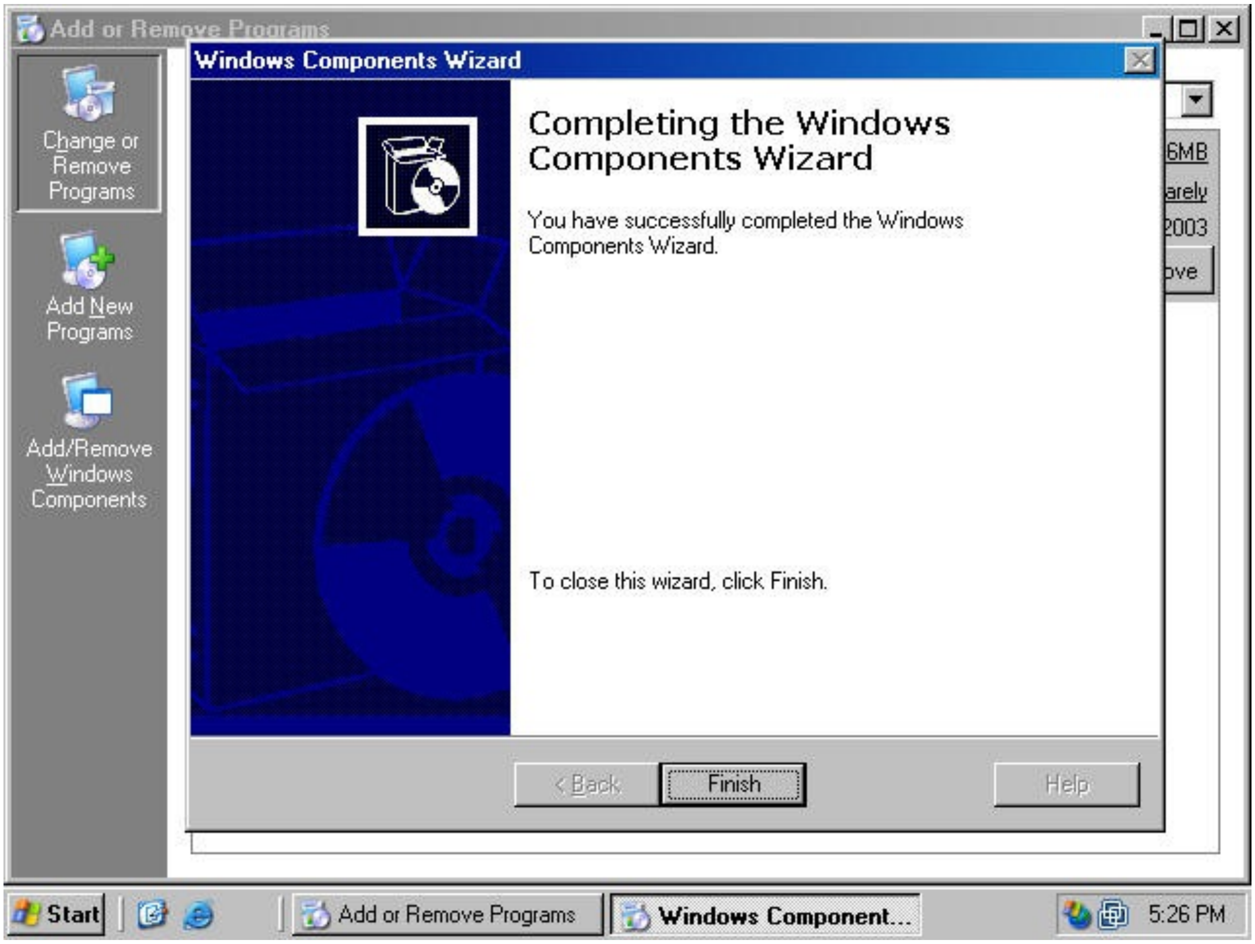
Description: Includes ASP.NET, Internet Information Services (IIS), and the Application Server Console.

Total disk space required: 14.1 MB

Space available on disk: 1943.5 MB

8. Click **Finish** on the **Completing the Windows Components Wizard** page (figure 7).

Figure 7


Completing the Windows Components Wizard

You have successfully completed the Windows Components Wizard.

To close this wizard, click Finish.

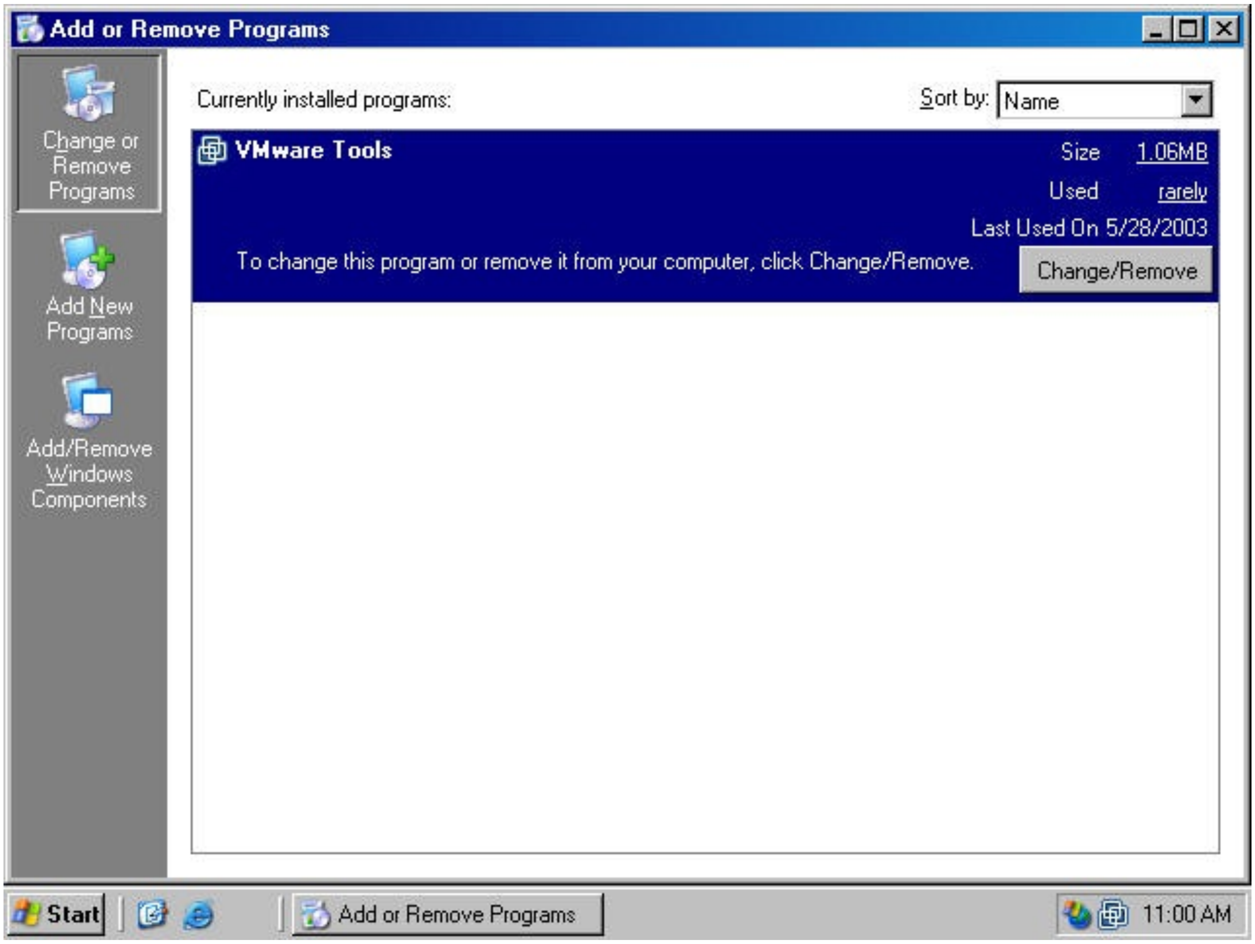
Installing Microsoft Certificate Services

Perform the following steps to install and configure a stand-alone CA on a Windows Server 2003 computer:

Note:
We recommend that you install the stand-alone CA on a member server or domain controller on your internal network. This allows the standalone Certificate Authority's CA certificate to be automatically placed in the Trusted Root Certification Authorities certificate store for all users and computers in the domain.

1. At a member server or domain controller in your internal network, log on as a domain administrator. Click **Start**, point to **Control Panel** and click **Add/Remove Programs**.
2. In the **Add or Remove Programs** window (figure 8), click the **Add/Remove Windows Components** button.

Figure 8



Currently installed programs:

Sort by: Name

VMware Tools

Size 1.06MB

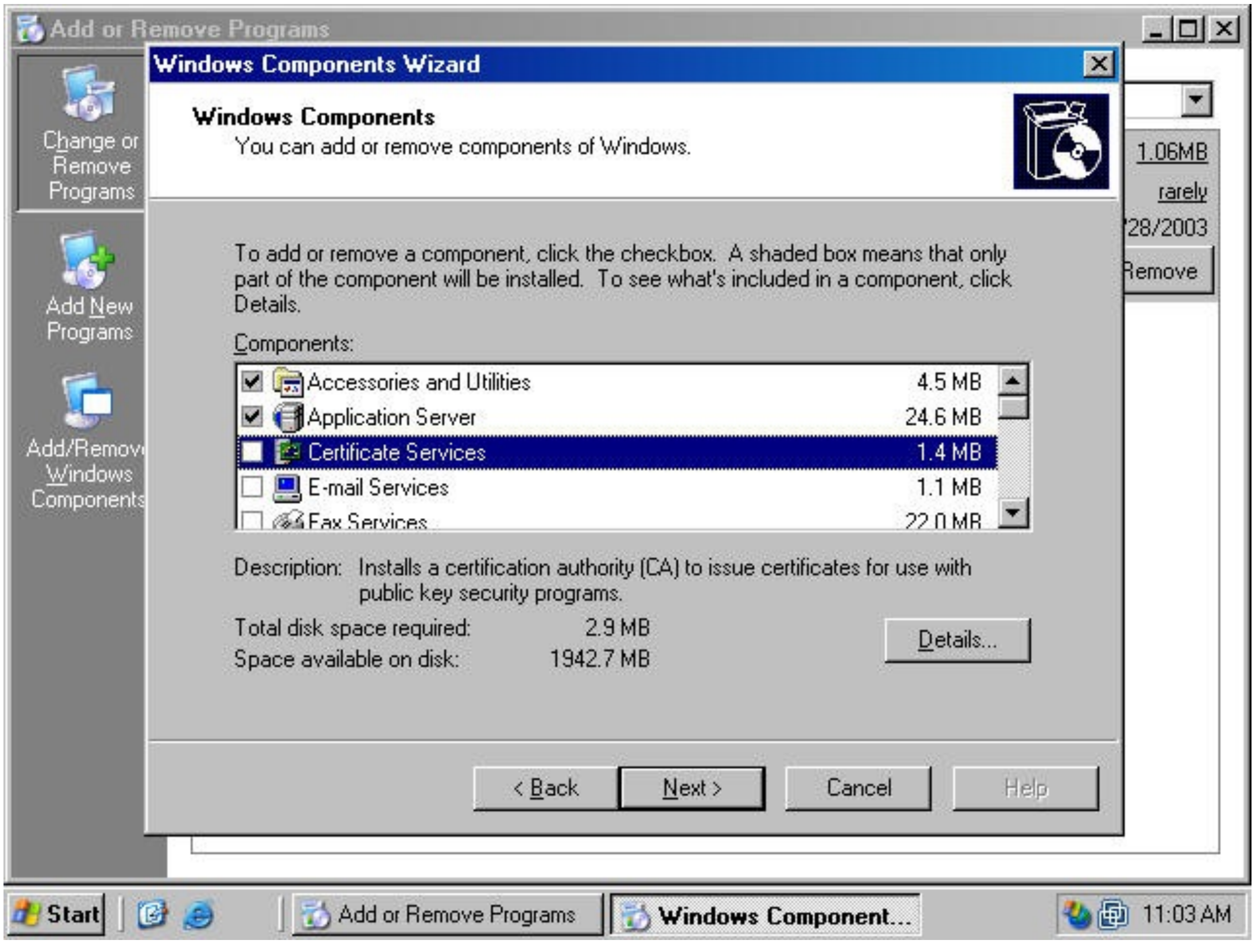
Used rarely

Last Used On 5/28/2003

To change this program or remove it from your computer, click Change/Remove.

3. In the **Windows Components** dialog box (figure 9), click on the **Certificate Services** entry and click the **Details** button.

Figure 9



Windows Components Wizard

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:

☑	Accessories and Utilities	4.5 MB
☑	Application Server	24.6 MB
□	Certificate Services	1.4 MB
□	E-mail Services	1.1 MB
□	Fax Services	22.0 MB

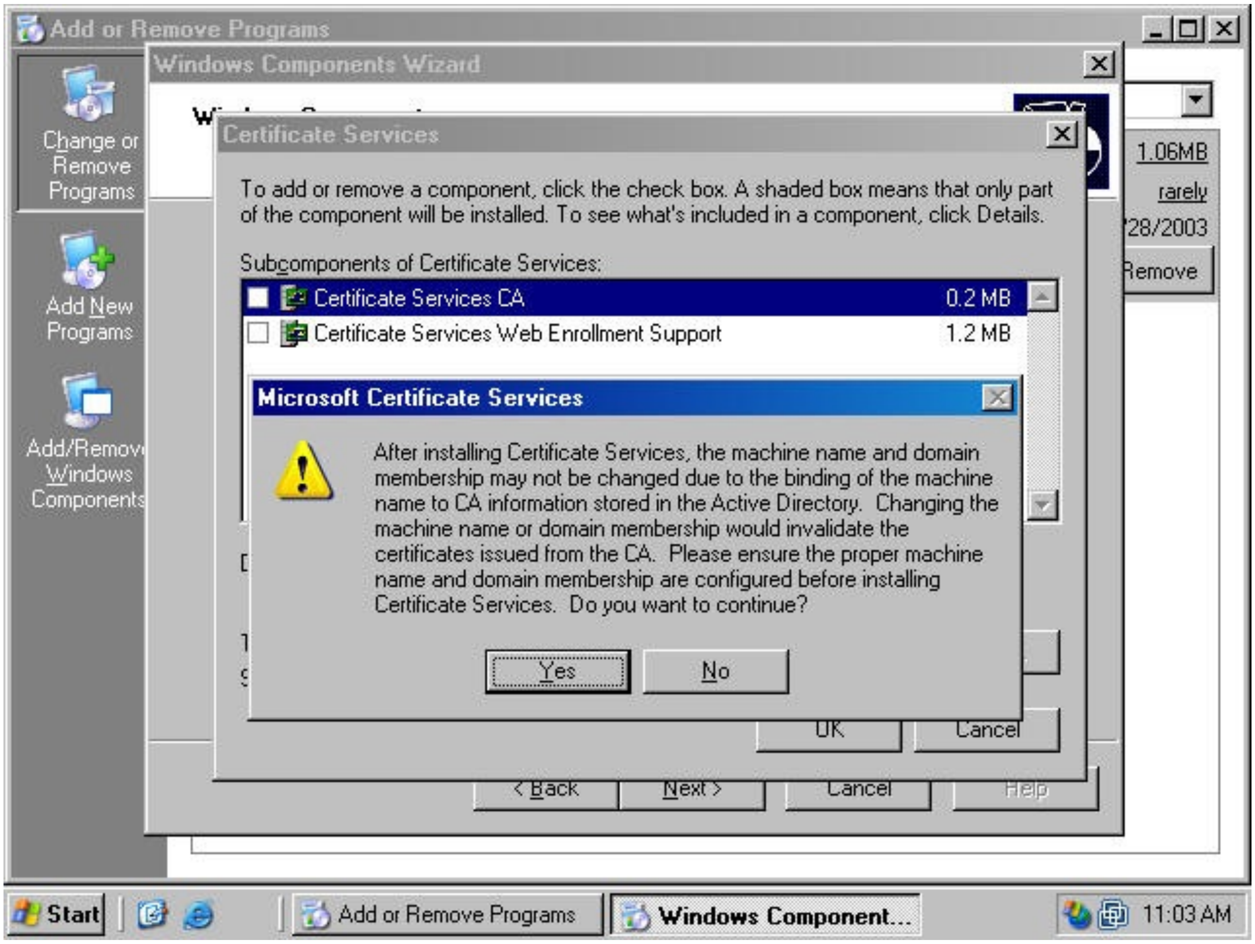
Description: Installs a certification authority (CA) to issue certificates for use with public key security programs.

Total disk space required: 2.9 MB

Space available on disk: 1942.7 MB

4. In the **Certificate Services** dialog box, put a checkmark in the **Certificate Services CA** checkbox (figure 10). A **Microsoft Certificate Services** dialog box appears and informs you that you can not change the machine name or the domain membership of the machine while it acts as a certificate server. Read the information in the dialog box and click **Yes**.

Figure 10



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

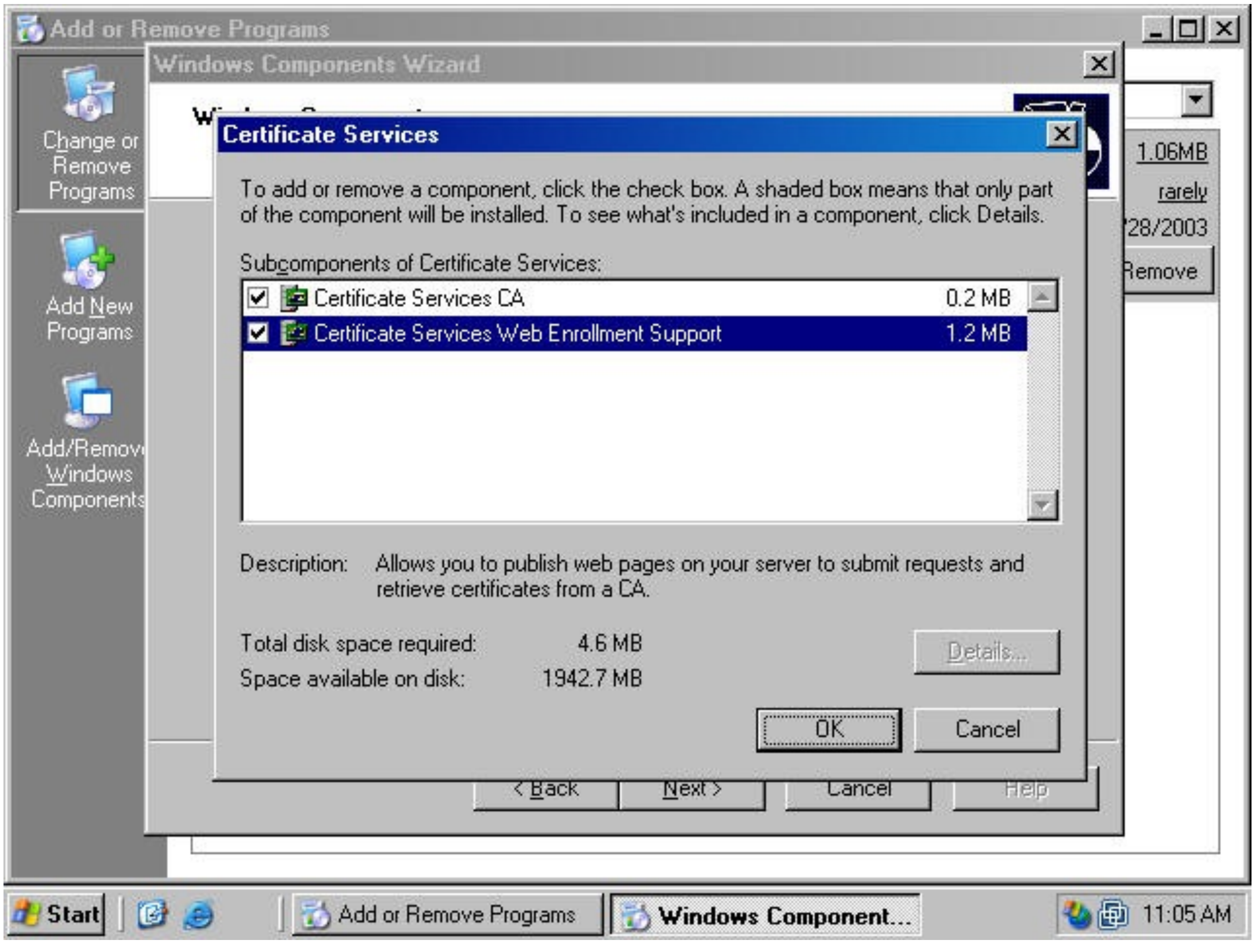
Subcomponents of Certificate Services:

- □ Certificate Services CA 0.2 MB
- □ Certificate Services Web Enrollment Support 1.2 MB

After installing Certificate Services, the machine name and domain membership may not be changed due to the binding of the machine name to CA information stored in the Active Directory. Changing the machine name or domain membership would invalidate the certificates issued from the CA. Please ensure the proper machine name and domain membership are configured before installing Certificate Services. Do you want to continue?

5. Both the **Certificate Services CA** and **Certificate Services Web Enrollment Support** checkboxes are checked (figure 11). Click **OK** in the **Certificate Services** dialog box.

Figure 11



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

Subcomponents of Certificate Services:

☑	Certificate Services CA	0.2 MB
☑	Certificate Services Web Enrollment Support	1.2 MB

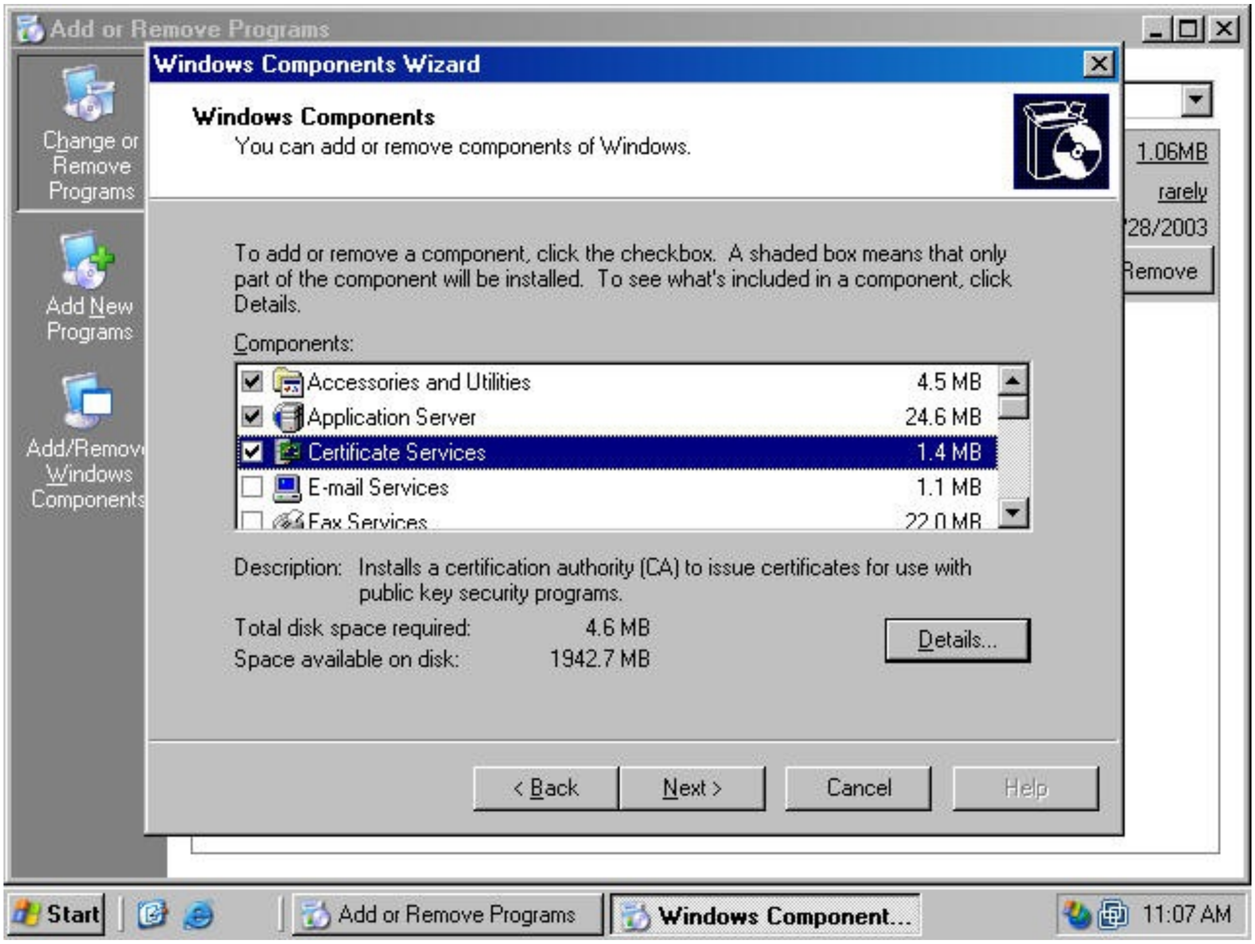
Description: Allows you to publish web pages on your server to submit requests and retrieve certificates from a CA.

Total disk space required: 4.6 MB

Space available on disk: 1942.7 MB

6. Click **Next** in the **Windows Components** dialog box (figure 12).

Figure 12



Windows Components Wizard

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:

☑	Accessories and Utilities	4.5 MB
☑	Application Server	24.6 MB
☑	Certificate Services	1.4 MB
□	E-mail Services	1.1 MB
□	Fax Services	22.0 MB

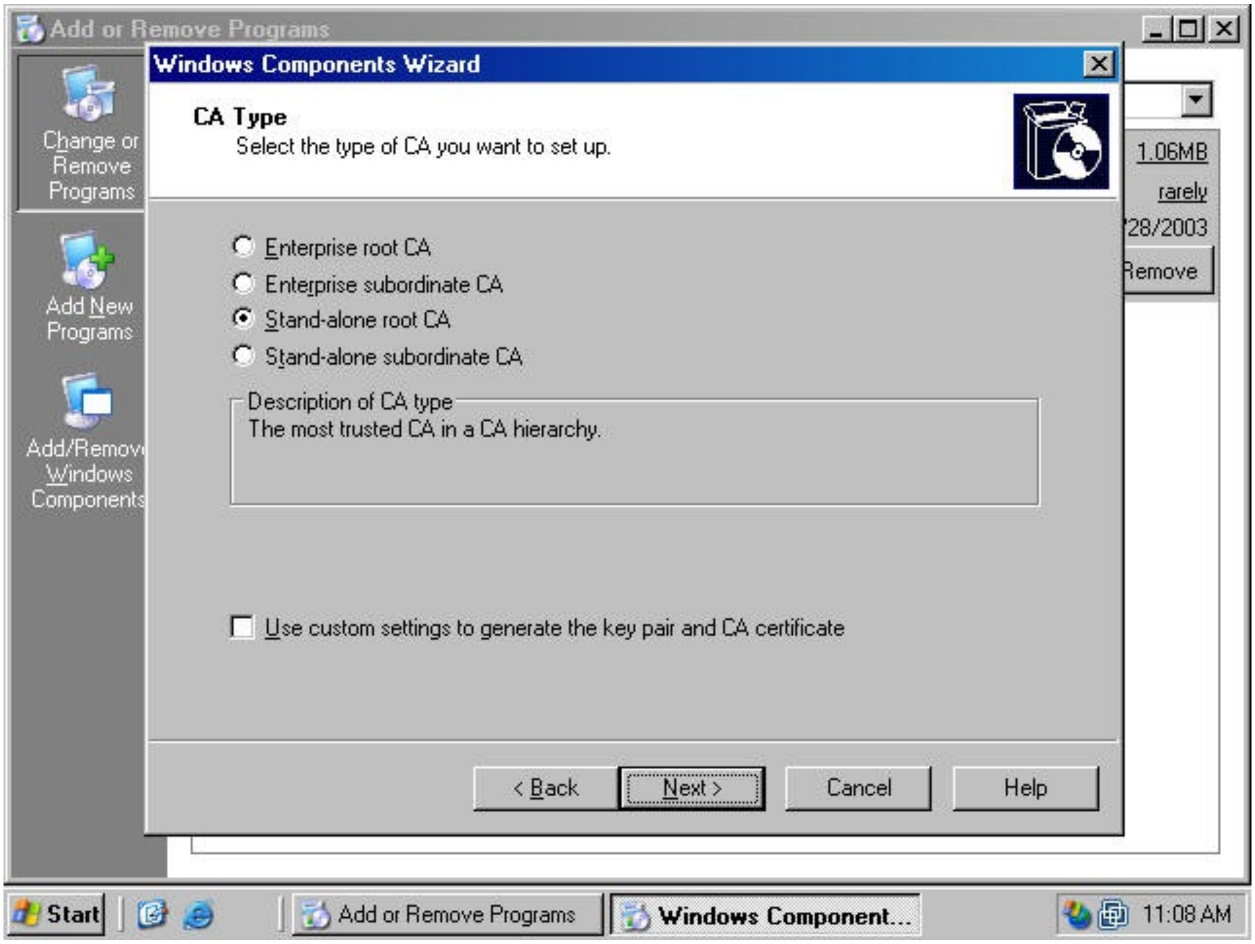
Description: Installs a certification authority (CA) to issue certificates for use with public key security programs.

Total disk space required: 4.6 MB

Space available on disk: 1942.7 MB

7. Select the **Stand-alone root CA** option on the **CA Type** page (figure 13). Click **Next**.

Figure 13



Windows Components Wizard

CA Type
Select the type of CA you want to set up.

○ Enterprise root CA
○ Enterprise subordinate CA
● Stand-alone root CA
○ Stand-alone subordinate CA

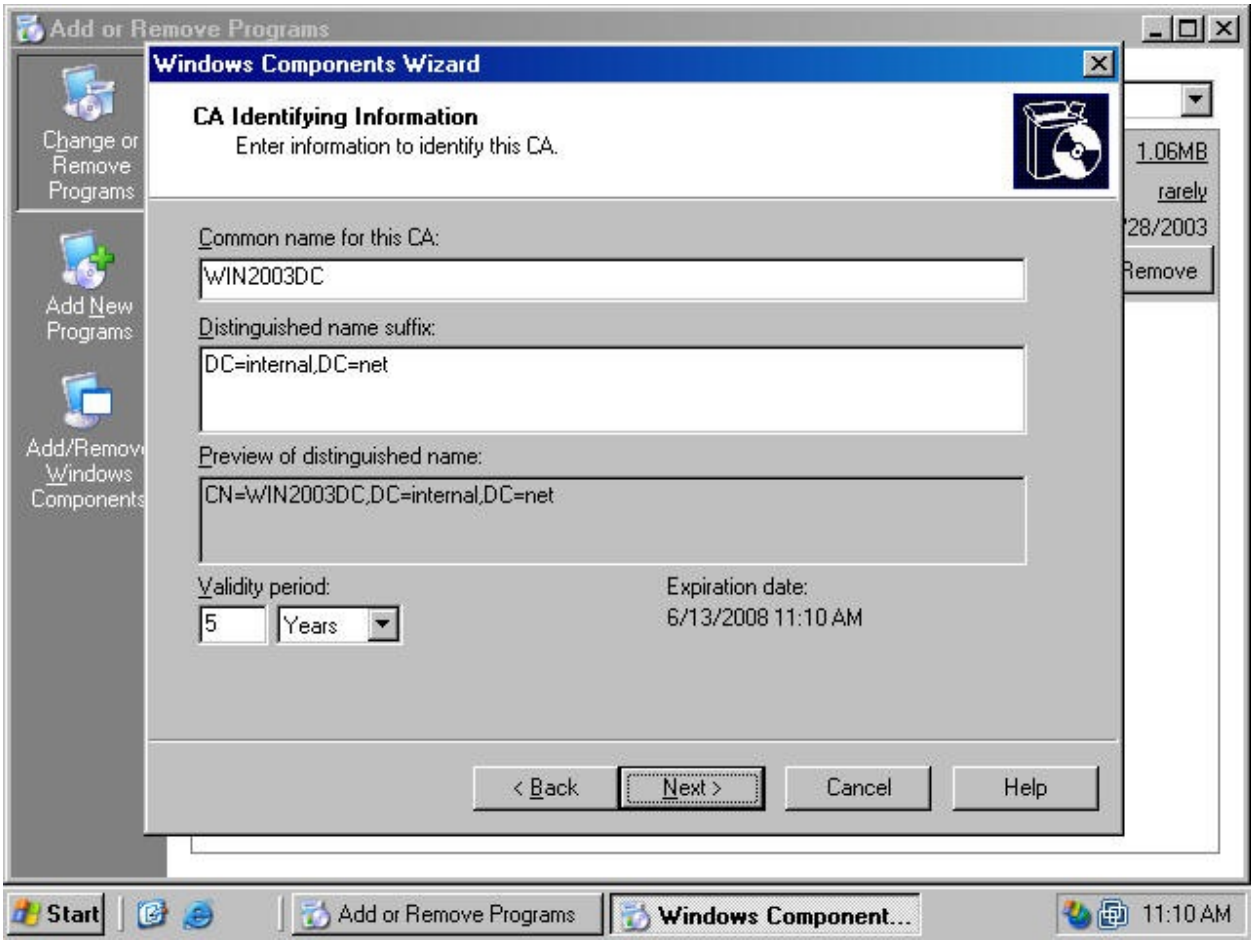
Description of CA type
The most trusted CA in a CA hierarchy.

□ Use custom settings to generate the key pair and CA certificate

< Back | Next > | Cancel | Help

8. On the **CA Identifying Information** page, type in a **Common name for this CA**. The common name of the CA is typically the DNS host name or NetBIOS name (computer name) of the machine running Certificate Services. In this example, the name of the machine is **WIN2003DC**, so we will enter **WIN2003DC** in the **Common name for this CA** text box. The default **Validity Period** of the CA's self-signed certificate is 5 years. Accept this default value unless you have a reason to change it. Click **Next**.

Figure 14



CA Identifying Information

Enter information to identify this CA.

Common name for this CA: WIN2003DC

Distinguished name suffix: DC=internal,DC=net

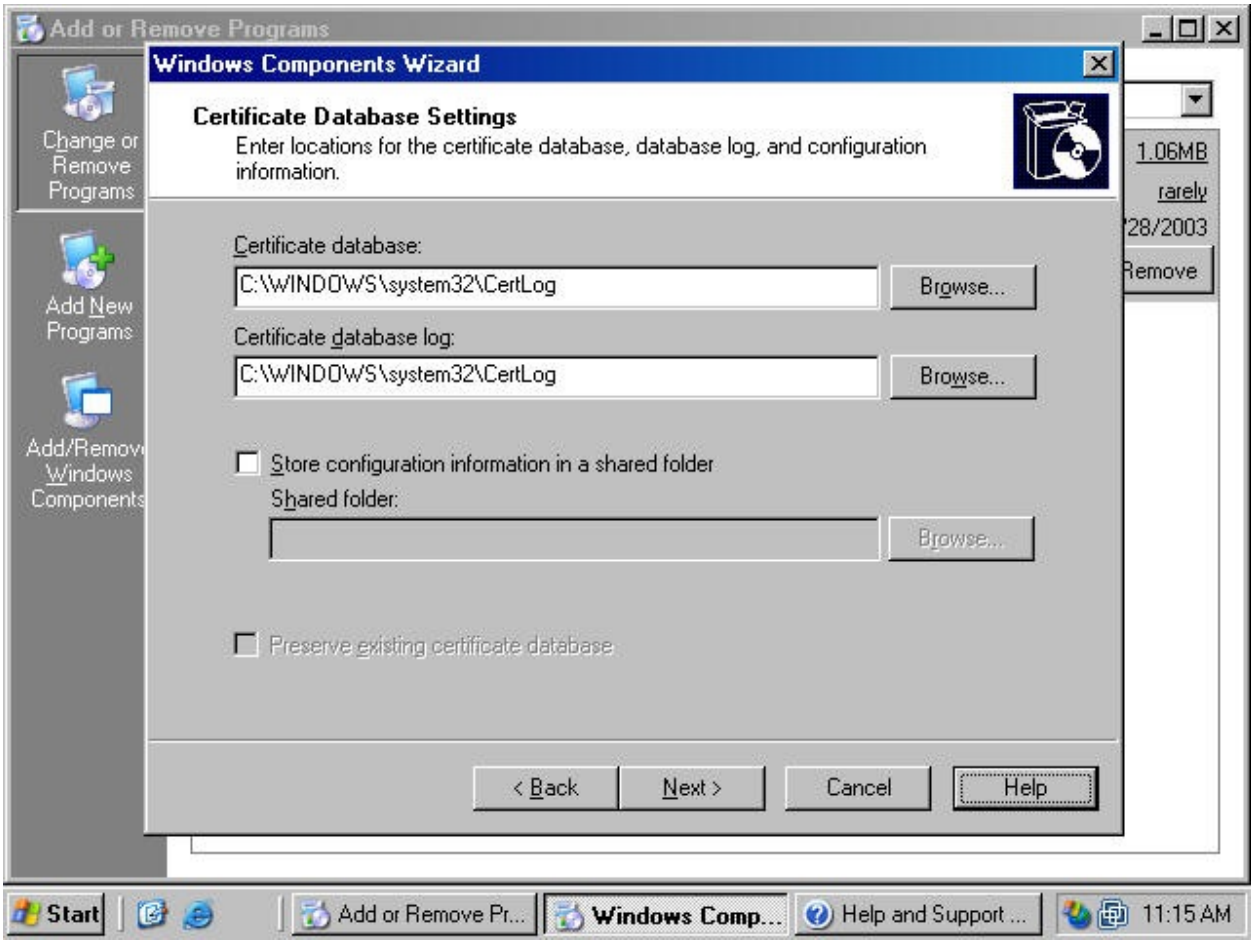
Preview of distinguished name: CN=WIN2003DC,DC=internal,DC=net

Validity period: 5 Years

Expiration date: 6/13/2008 11:10 AM

9. On the **Certificate Database Settings** page (figure 15), use the default locations for the **Certificate Database** and **Certificate Database Log**. You do not need to specify a shared folder to store configuration information because this information will be stored in the Active Directory. Click **Next**.

Figure 15



Windows Components Wizard

Certificate Database Settings

Enter locations for the certificate database, database log, and configuration information.

Certificate database: C:\WINDOWS\system32\CertLog

Certificate database log: C:\WINDOWS\system32\CertLog

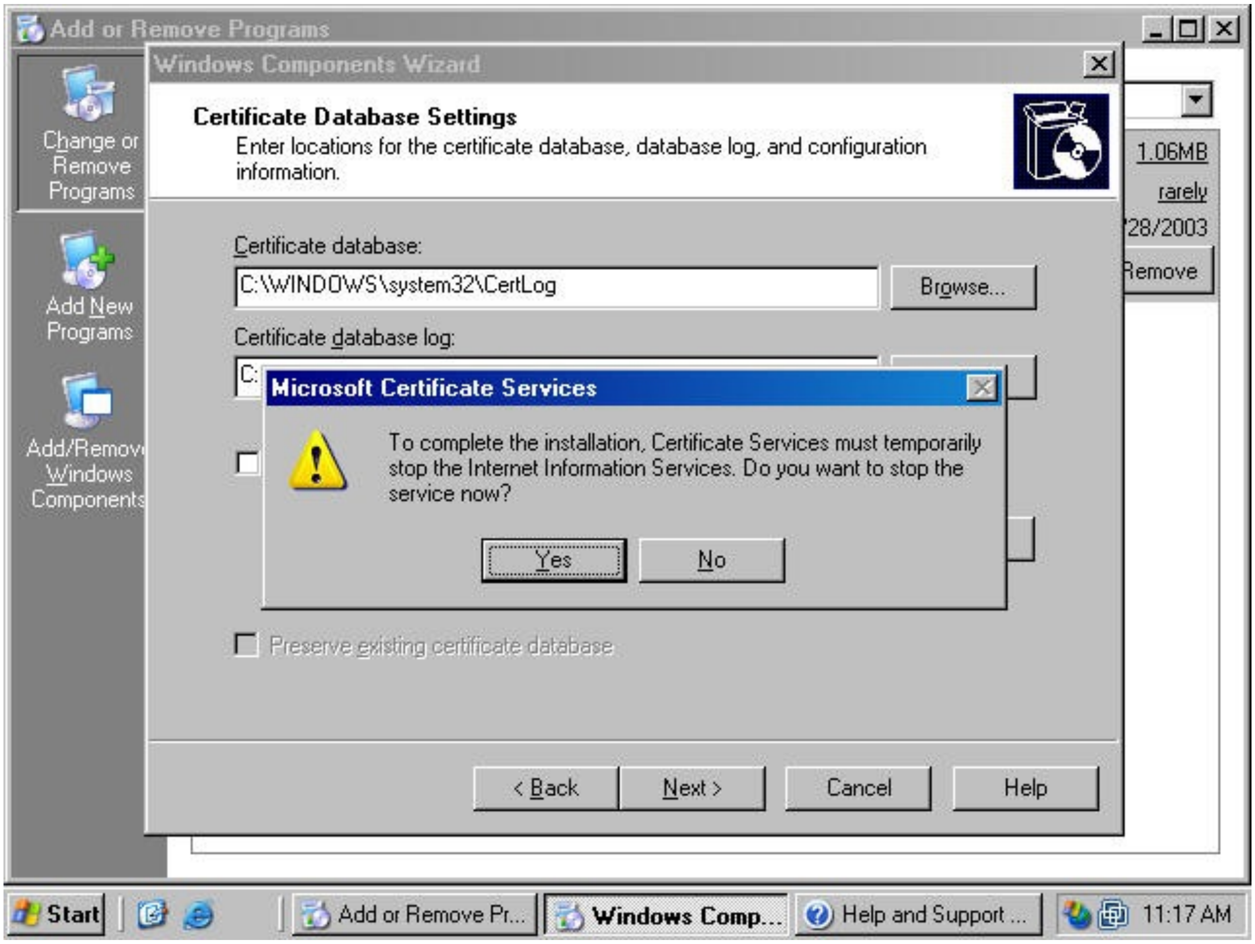
□ Store configuration information in a shared folder

Shared folder:

□ Preserve existing certificate database

10. Click **Yes** on the **Microsoft Certificate Services** dialog box (figure 16) informing you that Internet Information Services must be stopped temporarily.

Figure 16



Microsoft Certificate Services

To complete the installation, Certificate Services must temporarily stop the Internet Information Services. Do you want to stop the service now?

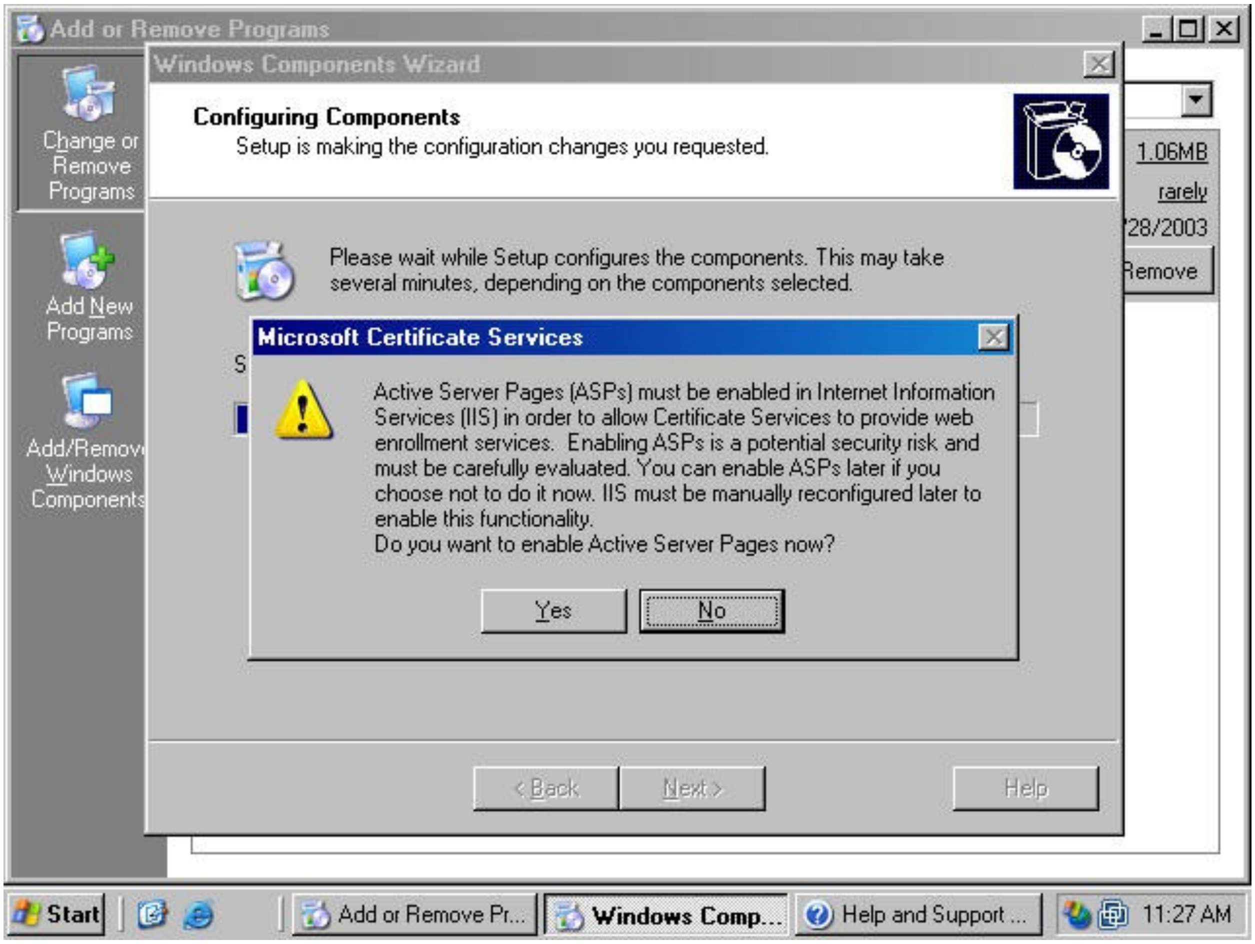
Certificate Database Settings

Enter locations for the certificate database, database log, and configuration information.

Certificate database: C:\WINDOWS\system32\CertLog

11. Click **Yes** on the **Microsoft Certificate Services** dialog box (figure 17) informing you that Active Server Pages must be enabled on IIS if you wish to use the Certificate Services Web enrollment site.

Figure 17



Configuring Components

Setup is making the configuration changes you requested.

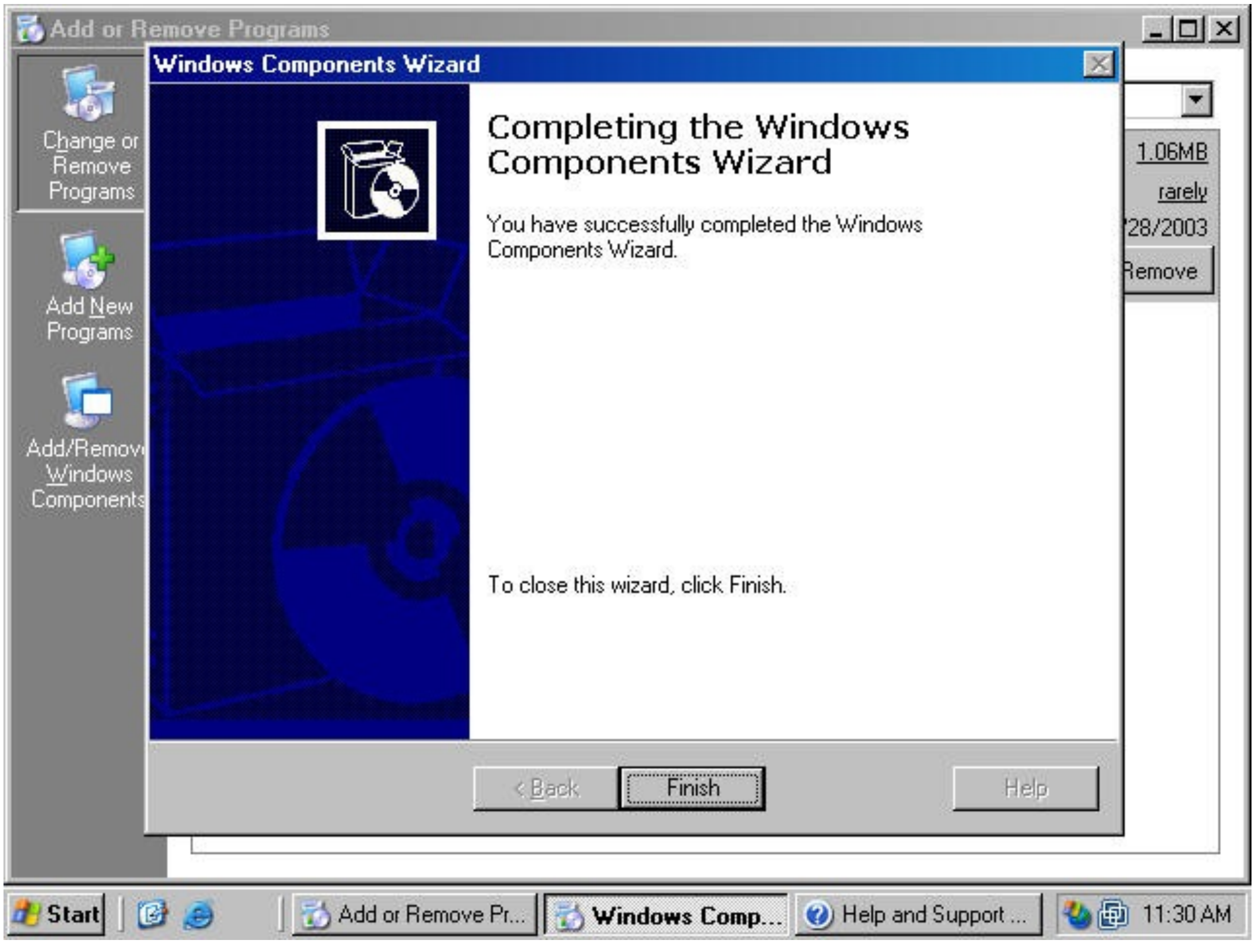
Please wait while Setup configures the components. This may take several minutes, depending on the components selected.

Microsoft Certificate Services

Active Server Pages (ASPs) must be enabled in Internet Information Services (IIS) in order to allow Certificate Services to provide web enrollment services. Enabling ASPs is a potential security risk and must be carefully evaluated. You can enable ASPs later if you choose not to do it now. IIS must be manually reconfigured later to enable this functionality.
Do you want to enable Active Server Pages now?

12. Click **Finish** on the **Completing the Windows Components Wizard** page (figure 18).

Figure 18



Completing the Windows Components Wizard

You have successfully completed the Windows Components Wizard.

To close this wizard, click Finish.

13. Close the **Add or Remove Programs** window.

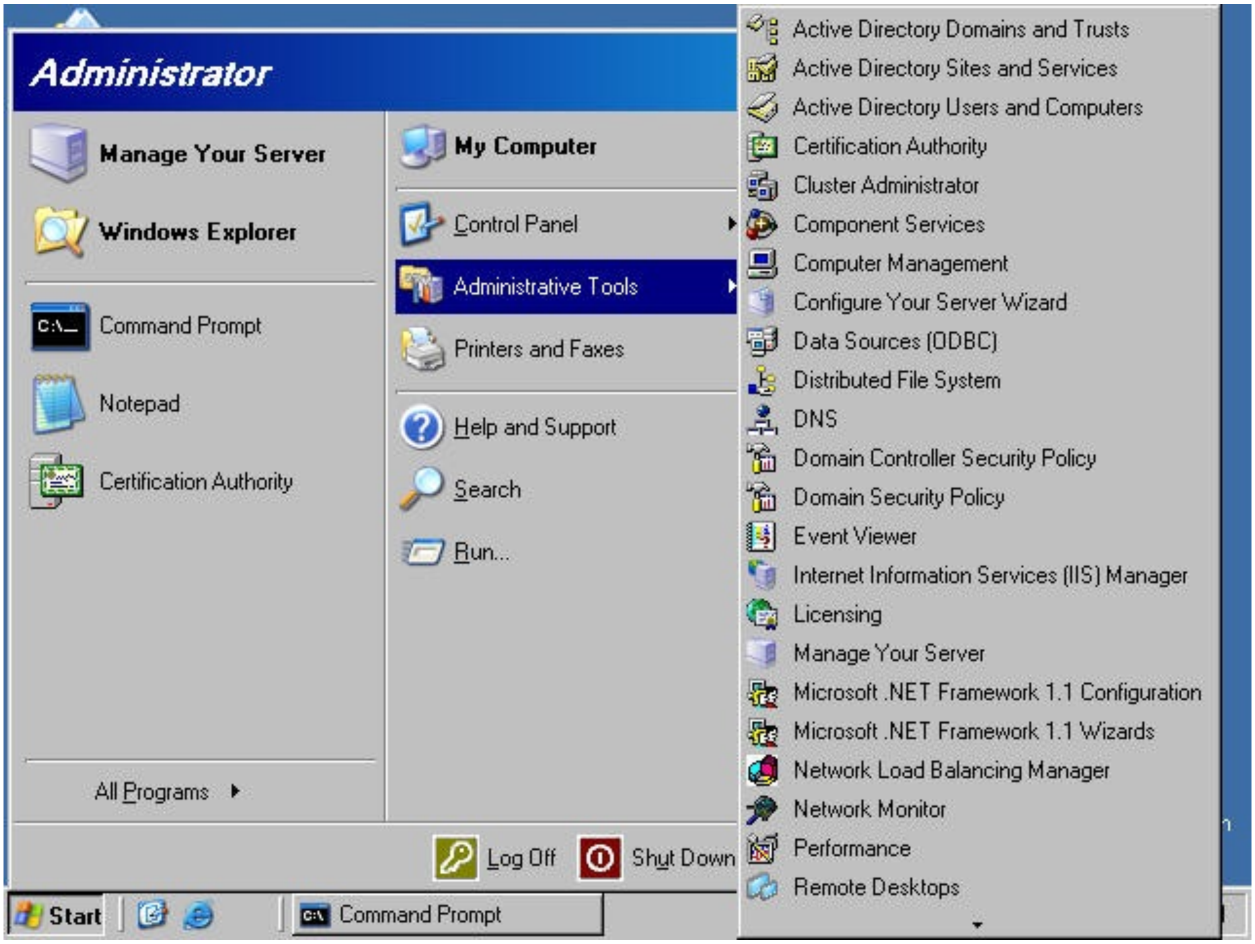
Approving Certificate Requests to a Standalone Certificate Authority

The stand-alone CA does not automatically issue a certificate when a certificate request is made. The reason is the standalone CA is not able to confirm the validity of the request. It does not check the information provided by the requestor against a directory, such as the enterprise CA does when validating credentials against the Active Directory.

You should keep this default behavior for your published standalone CA in order to prevent users on the Internet from obtaining certificates without your review. Perform the following steps to approve a certificate request:

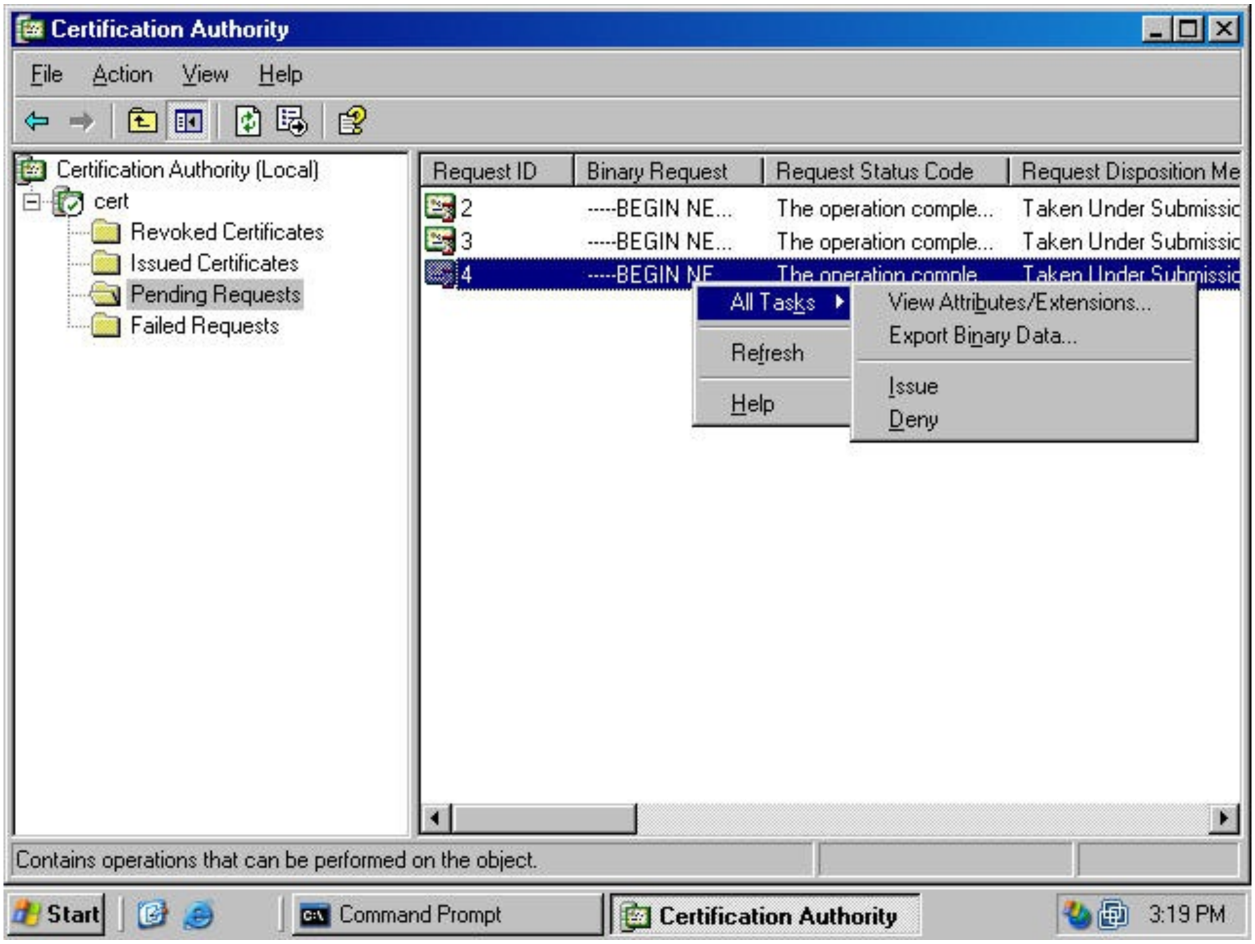
1. Click **Start** and point to **Administrative Tools**. Click on the **Certification Authority** link (figure 19).

Figure 19



2. In the **Certification Authority** console (figure 20), expand the server name and then click on the **Pending Certificates** node. You see a list of pending certificate requests in the right pane of the console. You can see who requested the certificate by scrolling to the right and looking under the **Requester Name** column (not shown). Right click on the certificate request in the right pane of the console, point to **All Tasks** and click **Issue**. The certificate request is removed from the **Pending Requests** node.

Figure 20

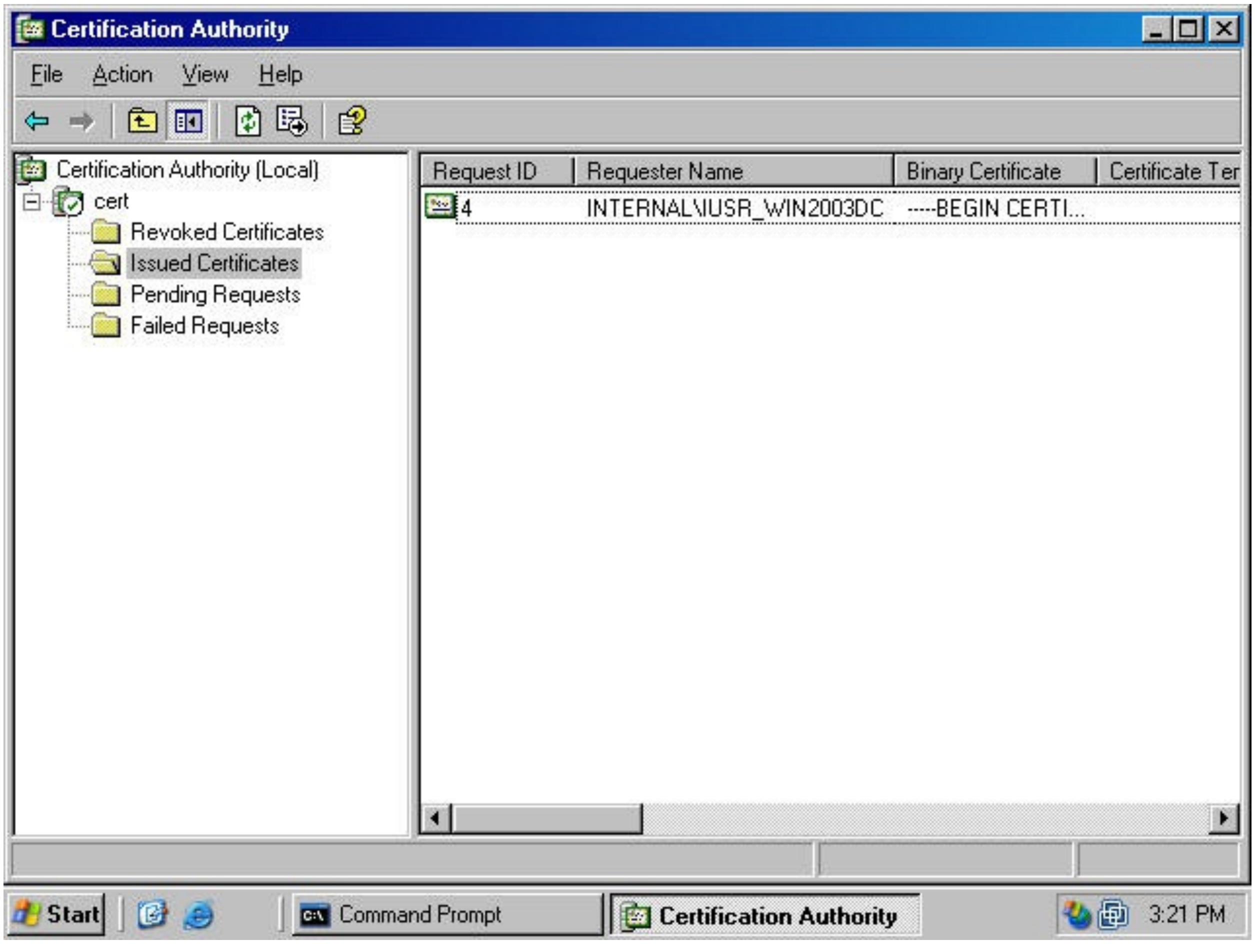


Request ID	Binary Request	Request Status Code	Request Disposition Me
2	-----BEGIN NE...	The operation comple...	Taken Under Submissic
3	-----BEGIN NE...	The operation comple...	Taken Under Submissic
4	-----BEGIN NE...	The operation comple...	Taken Under Submissic

Contains operations that can be performed on the object.

3. Click on the **Issued Certificates** node in the left pane of the **Certification Authority** console. The certificate request you approved appears in the right pane of the console. This indicates the certificate request was approved. It does not indicate the machine issuing the request has returned to the Web enrollment site to retrieve the certificate (figure 21).

Figure 21



Request ID	Requester Name	Binary Certificate	Certificate Ter
4	INTERNAL\IUSR_WIN2003DC	-----BEGIN CERTI...	

Identify the Location of the CA CRL and Configure the URLs for the Certificate Revocation List and Certificate Trust List

A certificate revocation list (CRL) is a list of certificates deemed invalid by Certificate Authority administrator. Clients and servers can use the CRL to check the validity of the certificate of the computer presenting a certificate. If the certificate is on the CRL, then the connection request can be denied. Making the CRL accessible to all hosts using certificates from the CA is critical in certificate authentication process.

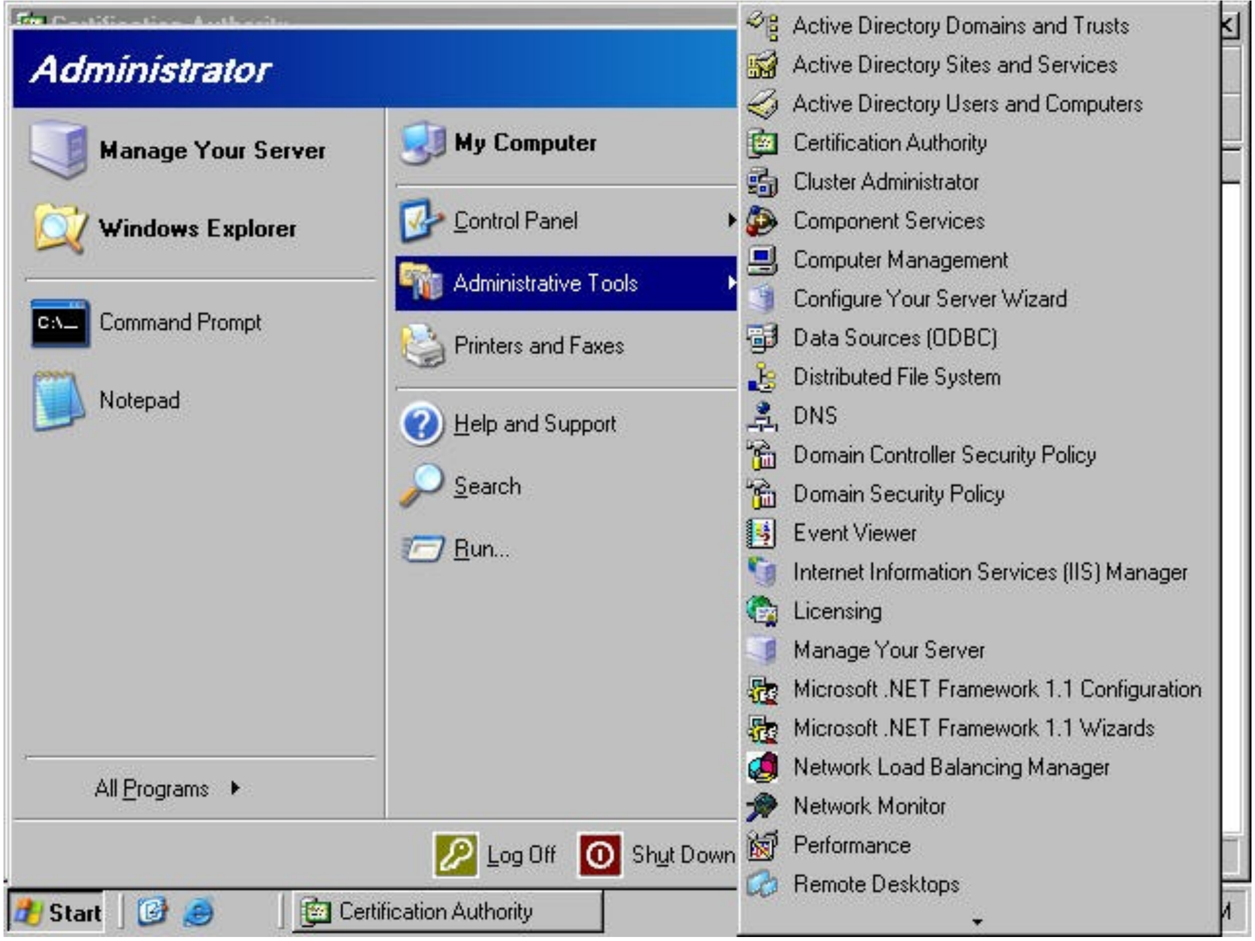
The location of the CRL is included in all certificates issued by the CA. When the VPN client connects to the VPN server, the VPN server can check the CRL to confirm that the VPN client’s certificate has not been revoked. The VPN client can also check the CRL to confirm the certificate issued to the VPN server has not been revoked.

You should also publish your Certificate Trust List (CTL). The CTL is a list of trusted Certificate Authorities. All participants in the certificate exchange process must trust the CA’s that issued the certificate of the opposite party. If one or both participants fail to trust the other’s certificate, then the certificate authentication process fails. Publishing the CTL makes it easy to import a list of trusted CAs into a client’s certificate store.

Perform the following steps identify the location of the CA CRL and configure URLs for the CRL and CTL:

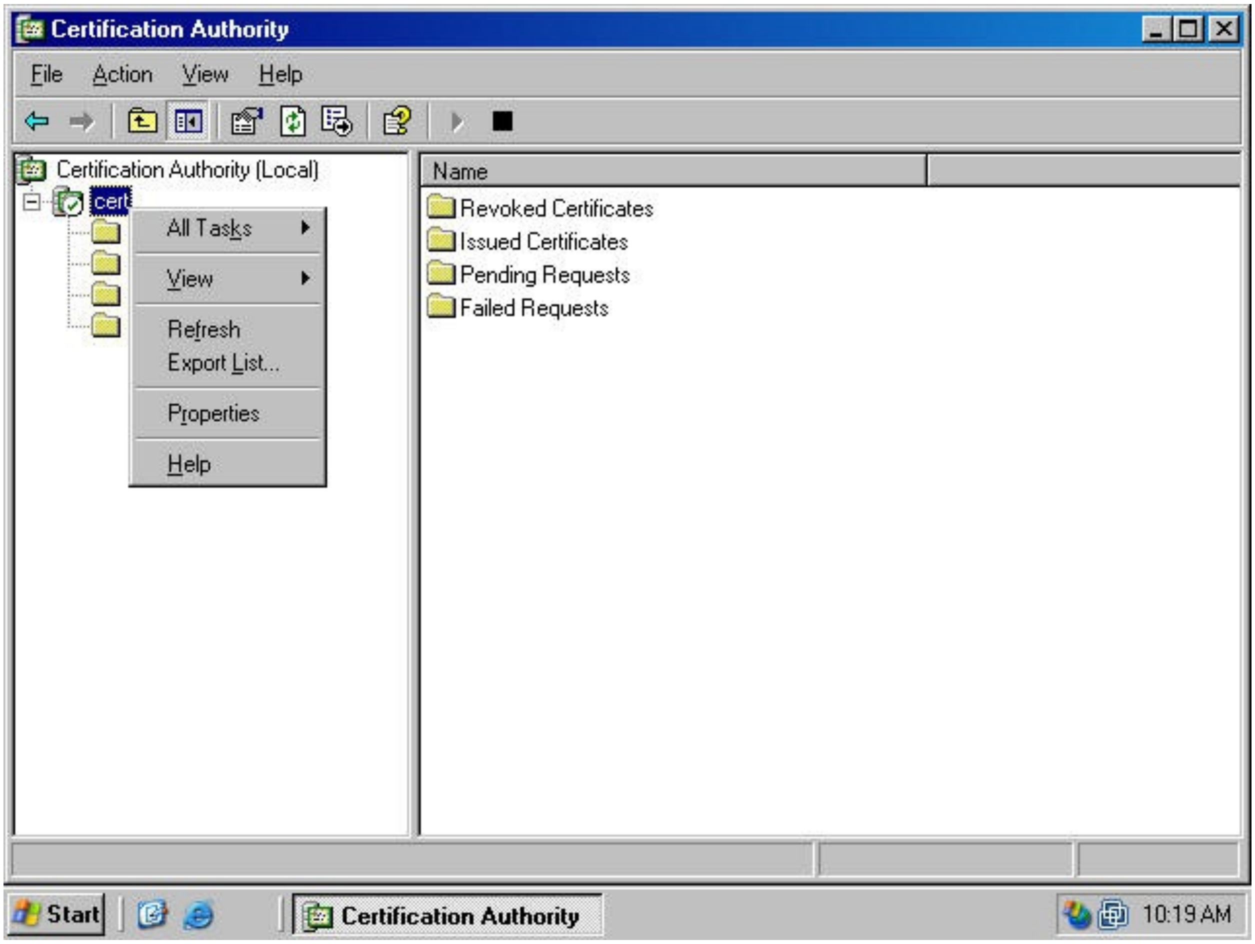
1. Click **Start**, point to **Administrative Tools** and click **Certification Authority** (figure 22).

Figure 22



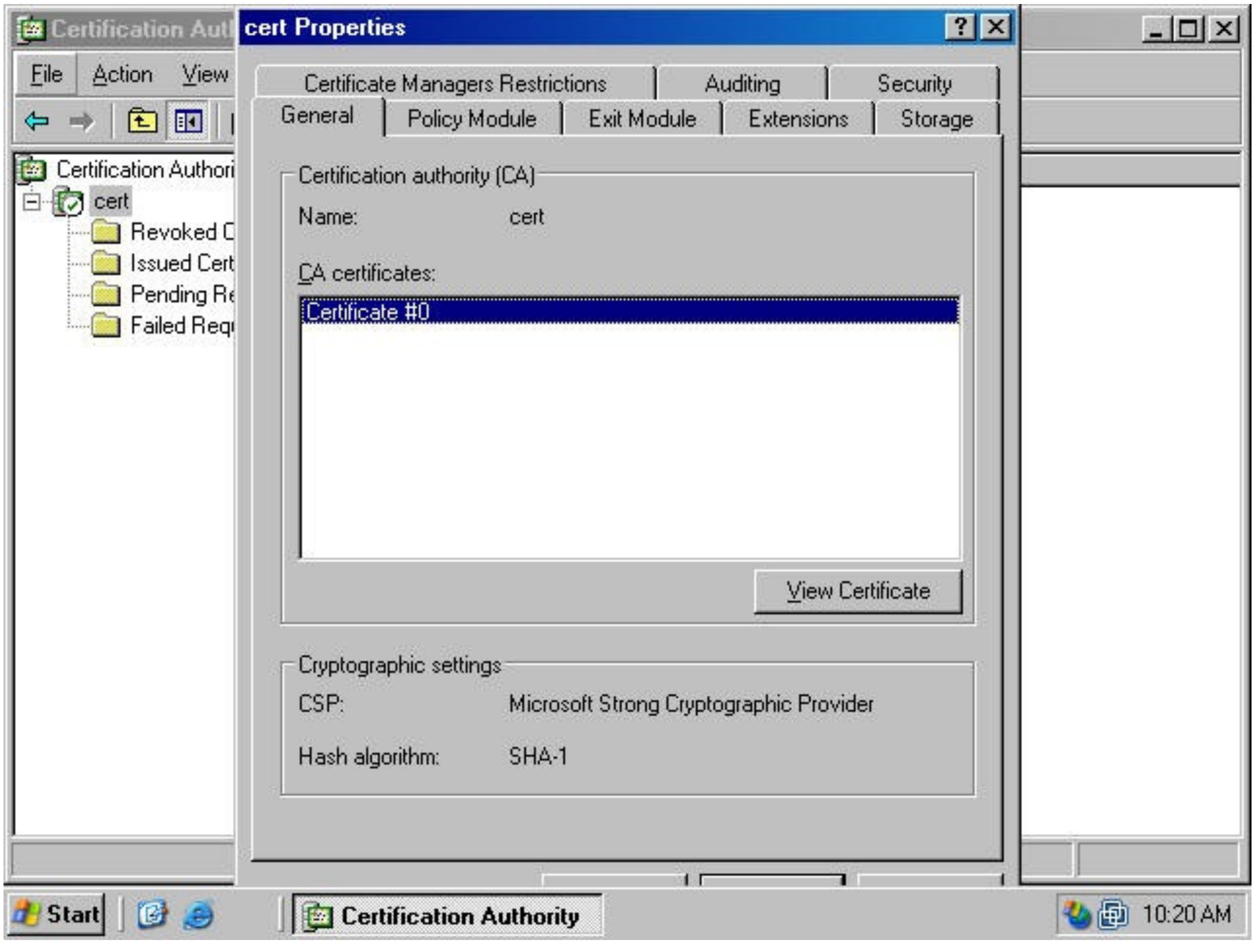
2. In the **Certification Authority** console, right click on the server name in the left pane of the console and click on **Properties** (figure 23).

Figure 23



3. In the server **Properties** dialog box (figure 24), click on the **General** tab. On the **General** tab, click on the **View Certificate** button.

Figure 24



Certification authority (CA)

Name: cert

CA certificates:

Certificate #0

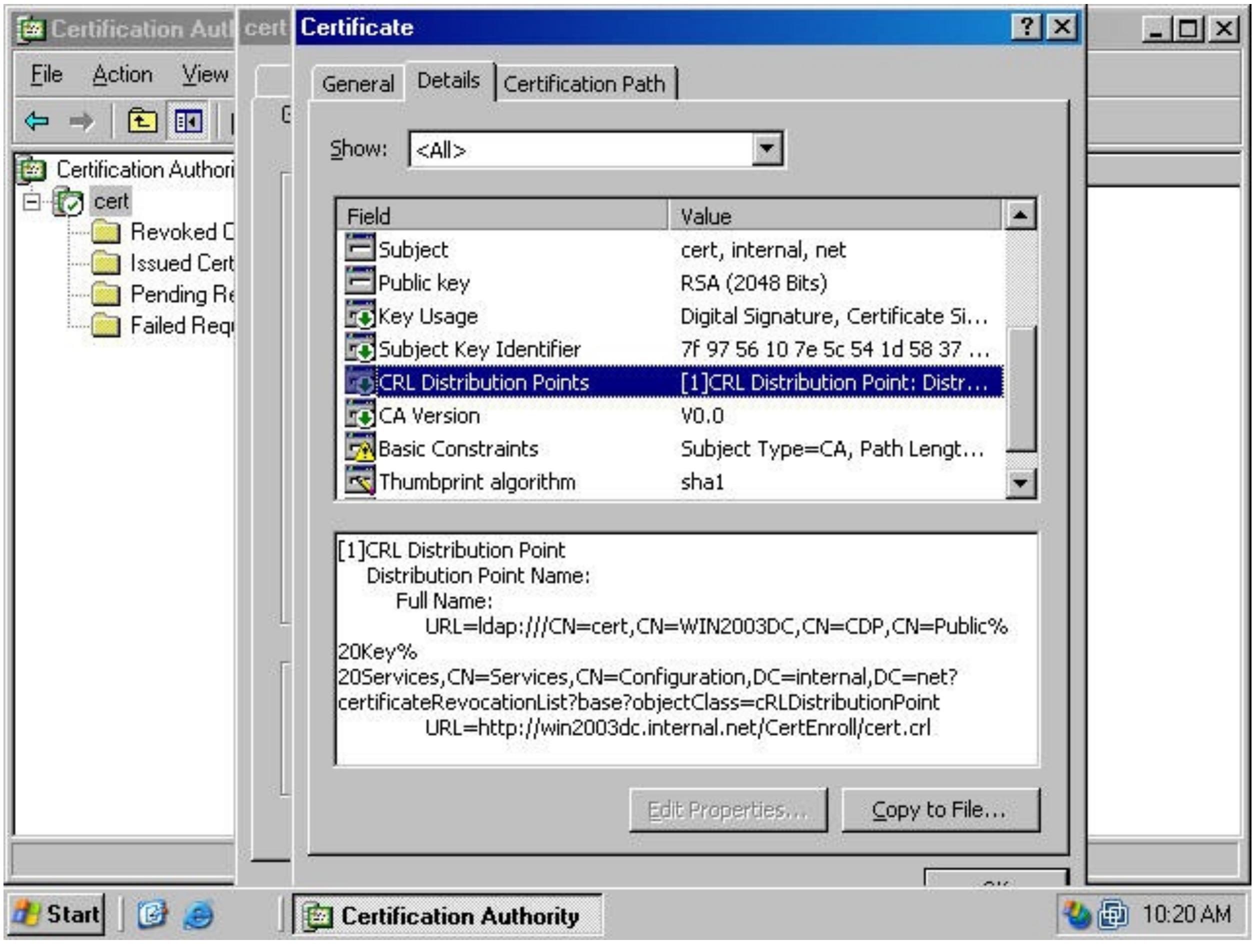
Cryptographic settings

CSP: Microsoft Strong Cryptographic Provider

Hash algorithm: SHA-1

4. Click the **Details** tab in the **Certificate** dialog box (figure 25). Scroll through the list of fields and find the **CRL Distribution Points** field. In the bottom pane of the **Certificate** dialog box you'll see the HTTP address of the CRL. In this example, the HTTP address is **http://win2003dc.internal.net/CertEnroll/cert.crl**. Write down the HTTP path. Click **OK**.

Figure 25



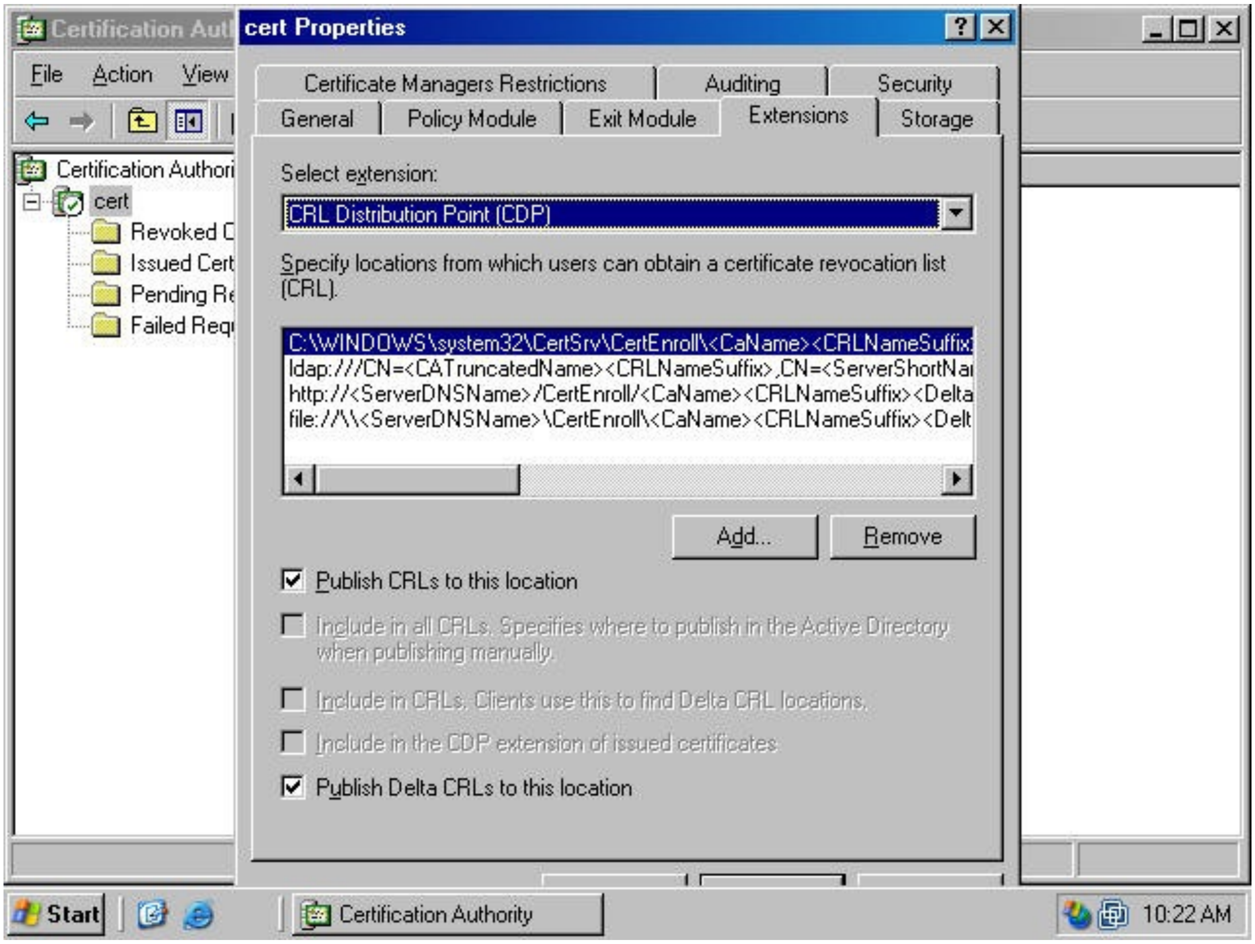
Field	Value
Subject	cert, internal, net
Public key	RSA (2048 Bits)
Key Usage	Digital Signature, Certificate Si...
Subject Key Identifier	7f 97 56 10 7e 5c 54 1d 58 37 ...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
CA Version	V0.0
Basic Constraints	Subject Type=CA, Path Lengt...
Thumbprint algorithm	sha1

```
[1]CRL Distribution Point
     Distribution Point Name:
          Full Name:
               URL=ldap:///CN=cert,CN=WIN2003DC,CN=CDP,CN=Public%
20Key%
20Services,CN=Services,CN=Configuration,DC=internal,DC=net?
certificateRevocationList?base?objectClass=cRLDistributionPoint
               URL=http://win2003dc.internal.net/CertEnroll/cert.crl
```

5. Click the **Extensions** tab in the server **Properties** dialog box. Click the down arrow in the **Select extension** drop down list box and select **CRL Distribution Point (CDP)**. Find the HTTP path for the CDP in the list of location and click on it. Find the entry in the list that begins with HTTP.

   Select that entry and click the **Remove** button (figure 26).

Figure 26



Select extension:
CRL Distribution Point (CDP)

Specify locations from which users can obtain a certificate revocation list (CRL).

```
C:\WINDOWS\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix>
ldap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortNa
http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><Delta
file://\\<ServerDNSName>\CertEnroll\<CaName><CRLNameSuffix><Delt
```

☑ Publish CRLs to this location

☐ Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.

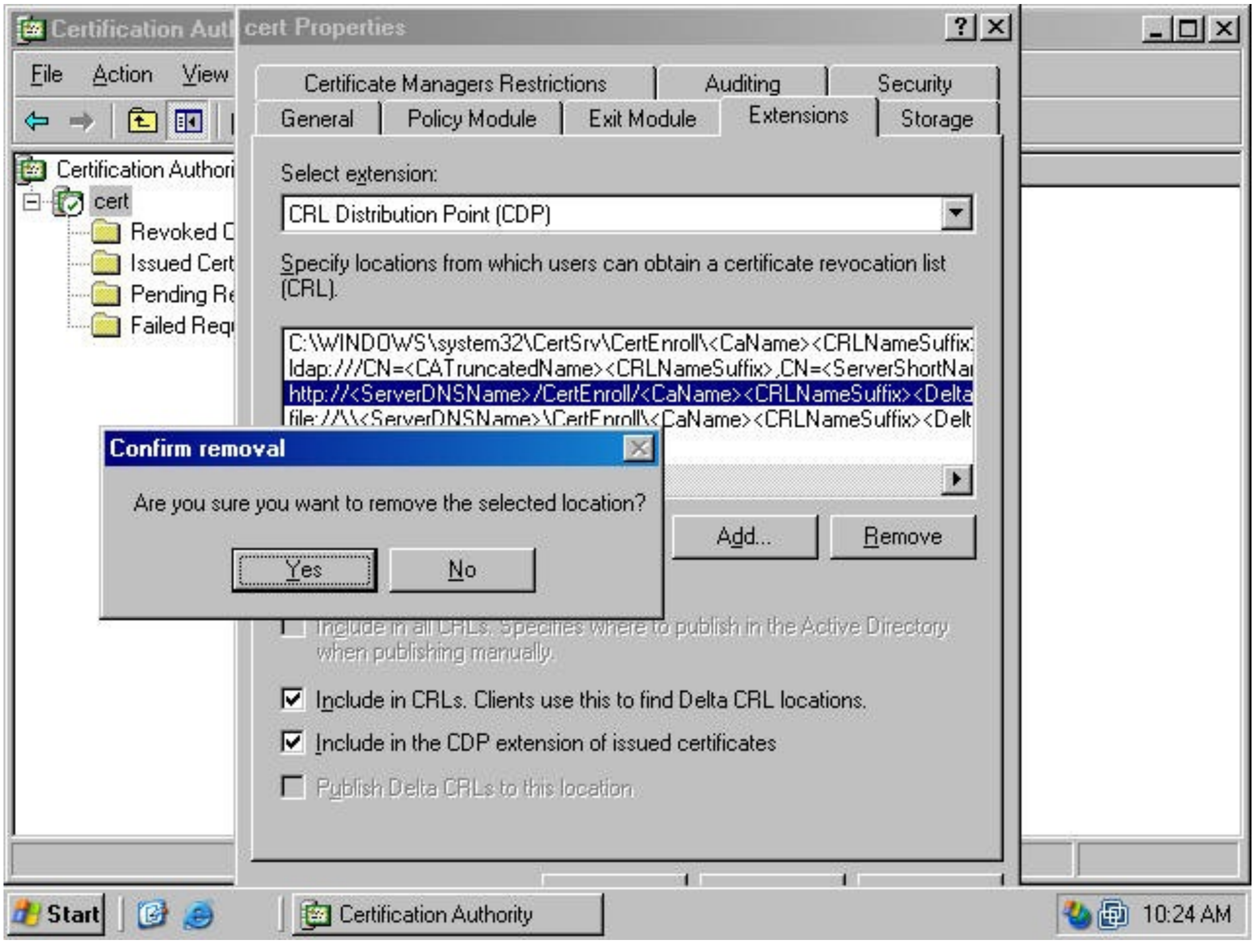
☐ Include in CRLs. Clients use this to find Delta CRL locations.

☐ Include in the CDP extension of issued certificates

☑ Publish Delta CRLs to this location

6. Click the **Yes** button in the **Confirm removal** dialog box (figure 27).

Figure 27



Select extension:

CRL Distribution Point (CDP)

Specify locations from which users can obtain a certificate revocation list (CRL).

```
C:\WINDOWS\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix:
ldap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortNa
http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><Delta
file://\\<ServerDNSName>\CertEnroll\<CaName><CRLNameSuffix><Delt
```

Confirm removal

Are you sure you want to remove the selected location?

Yes No

□ Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.

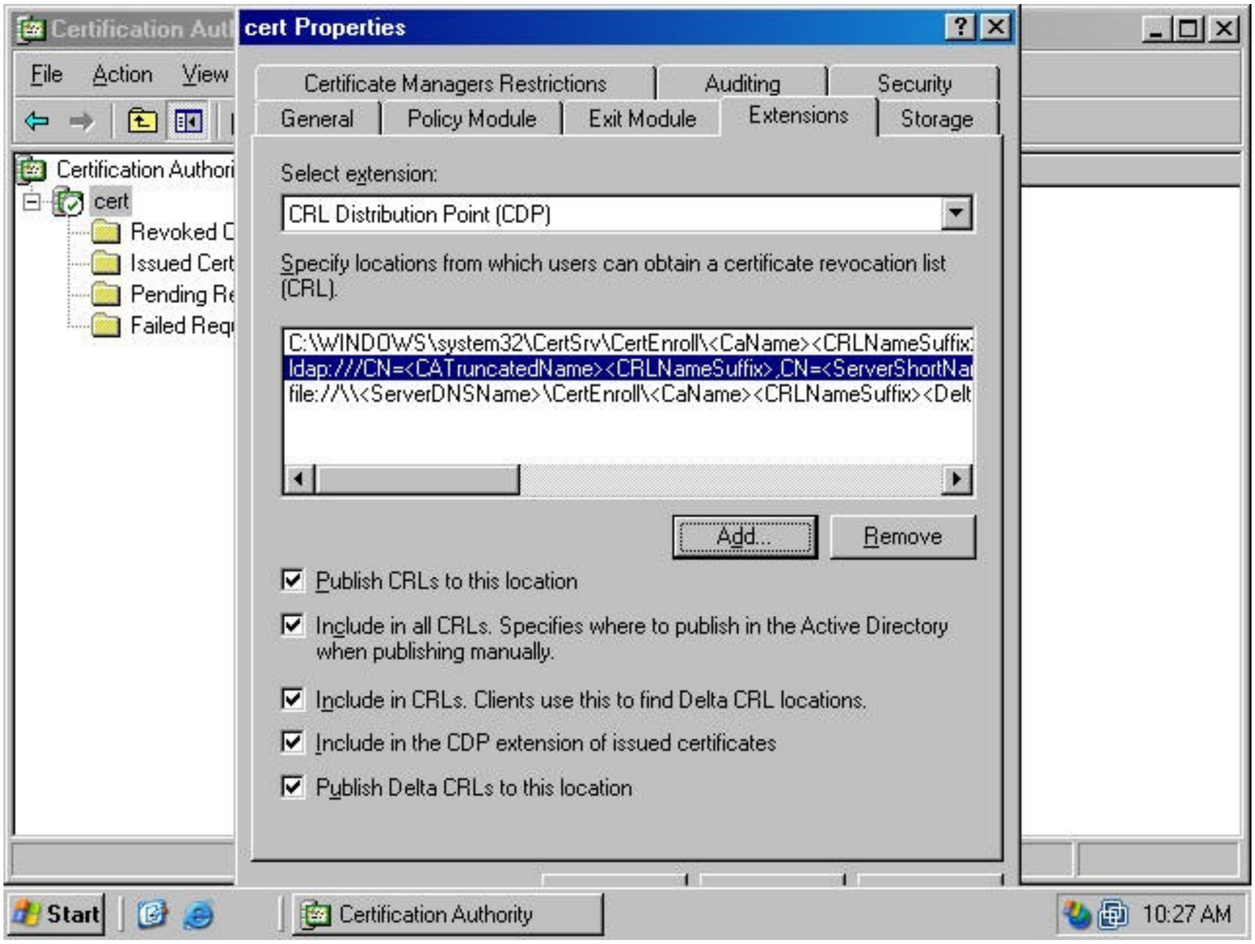
☑ Include in CRLs. Clients use this to find Delta CRL locations.

☑ Include in the CDP extension of issued certificates

□ Publish Delta CRLs to this location

7. Click the **Add** button on the **Extensions** tab (figure 28).

Figure 28



Select extension:

CRL Distribution Point (CDP)

Specify locations from which users can obtain a certificate revocation list (CRL).

```
C:\WINDOWS\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix:
ldap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortNa
file://\\<ServerDNSName>\CertEnroll\<CaName><CRLNameSuffix><Delt
```

☑ Publish CRLs to this location

☑ Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.

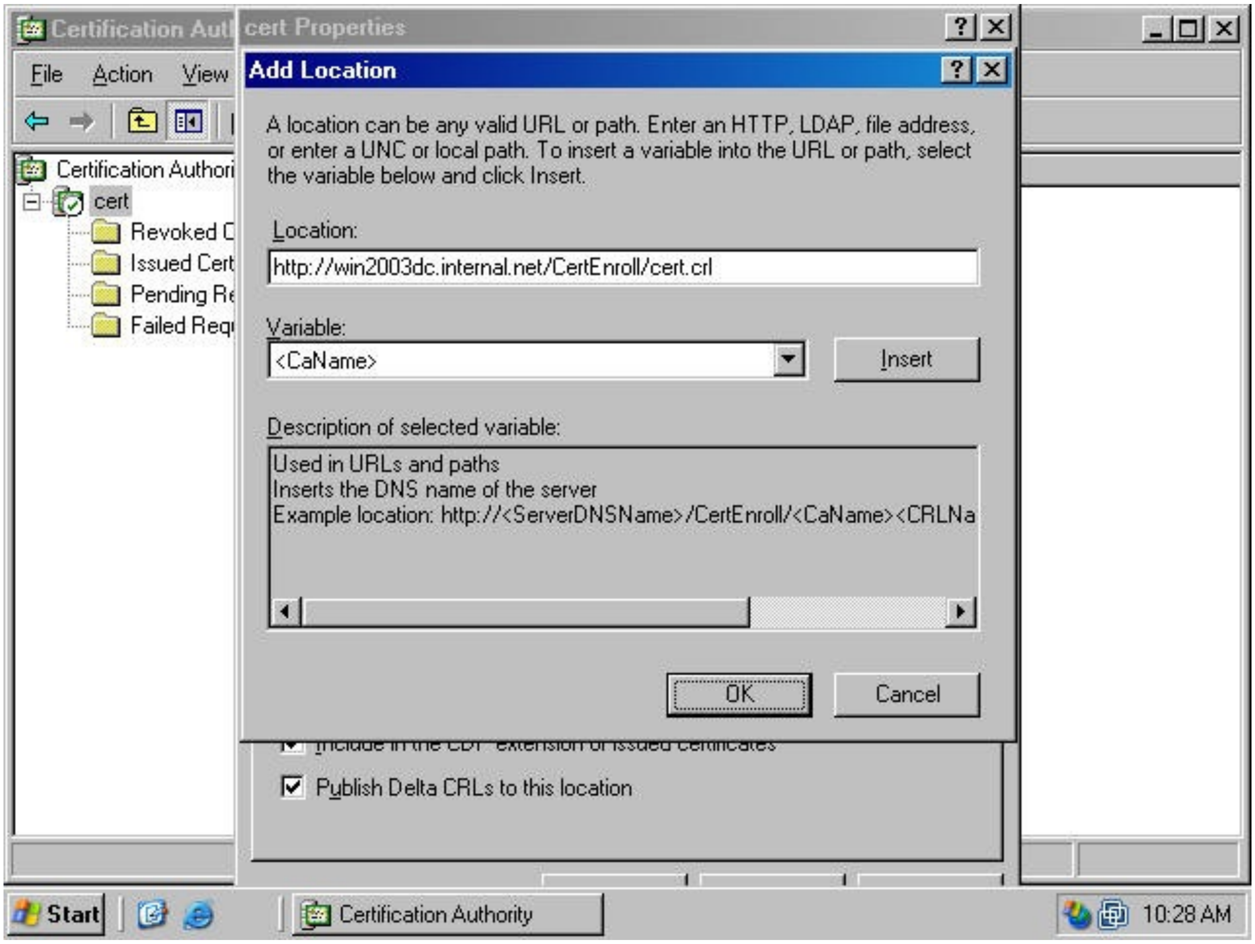
☑ Include in CRLs. Clients use this to find Delta CRL locations.

☑ Include in the CDP extension of issued certificates

☑ Publish Delta CRLs to this location

8. In the **Location** text box, type in the HTTP to the CRL. This is the path we wrote down in step 4 (figure 29). Click **OK**.

Figure 29



Add Location

A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.

Location: http://win2003dc.internal.net/CertEnroll/cert.crl

Variable: <CaName>

Description of selected variable:

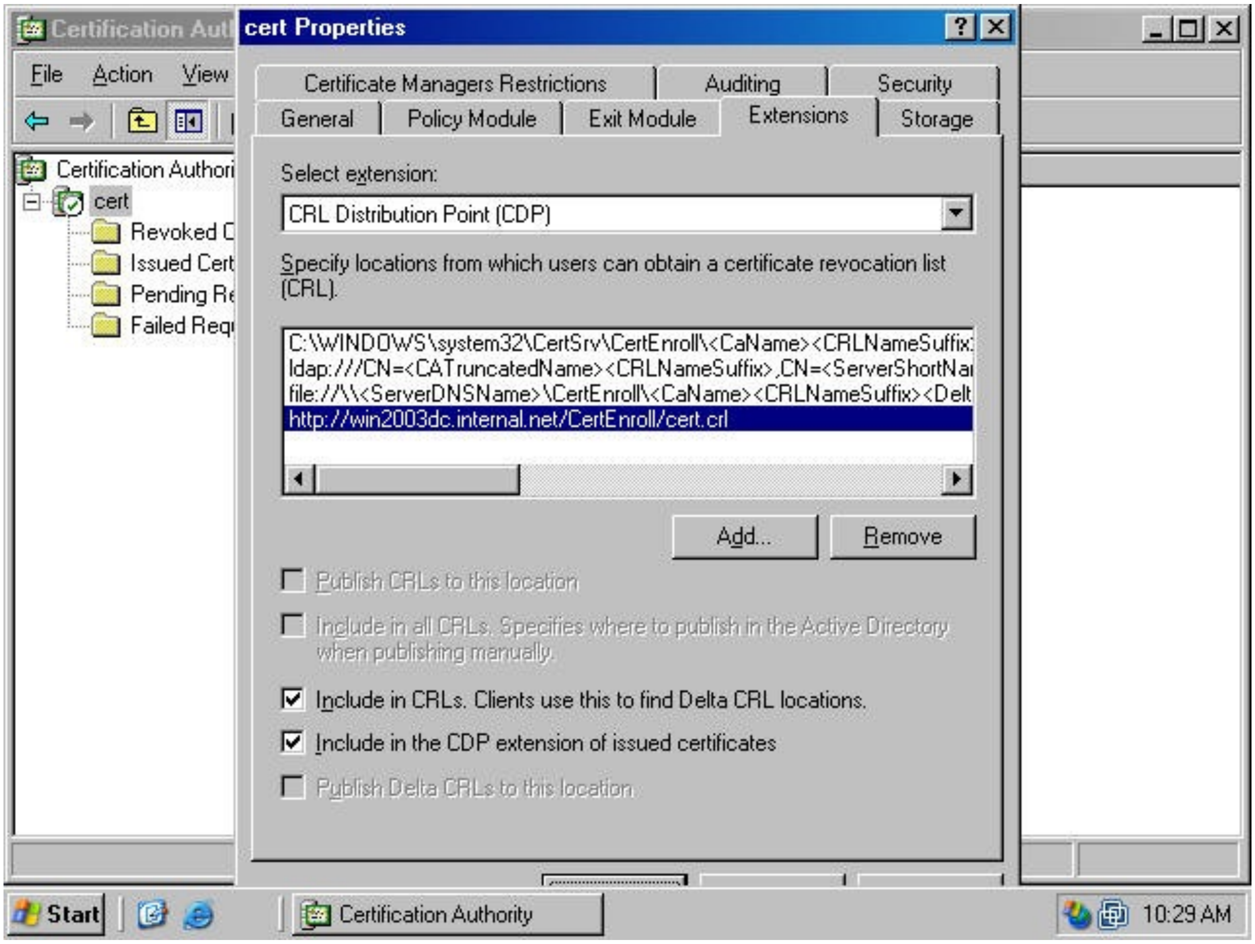
Used in URLs and paths
Inserts the DNS name of the server
Example location: http://<ServerDNSName>/CertEnroll/<CaName><CRLNa

☑ Include in the CDP extension of issued certificates

☑ Publish Delta CRLs to this location

9. Put a checkmark in the **Include in CRLs. Clients use this to find Delta CRL locations** and **Include in the CDP extension of issued certificates** checkboxes (figure 30). Click **Apply**.

Figure 30



Select extension:

CRL Distribution Point (CDP)

Specify locations from which users can obtain a certificate revocation list (CRL).

```
C:\WINDOWS\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix:
ldap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortNa
file://\\<ServerDNSName>\CertEnroll\<CaName><CRLNameSuffix><Delt
http://win2003dc.internal.net/CertEnroll/cert.crl
```

☐ Publish CRLs to this location

☐ Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.

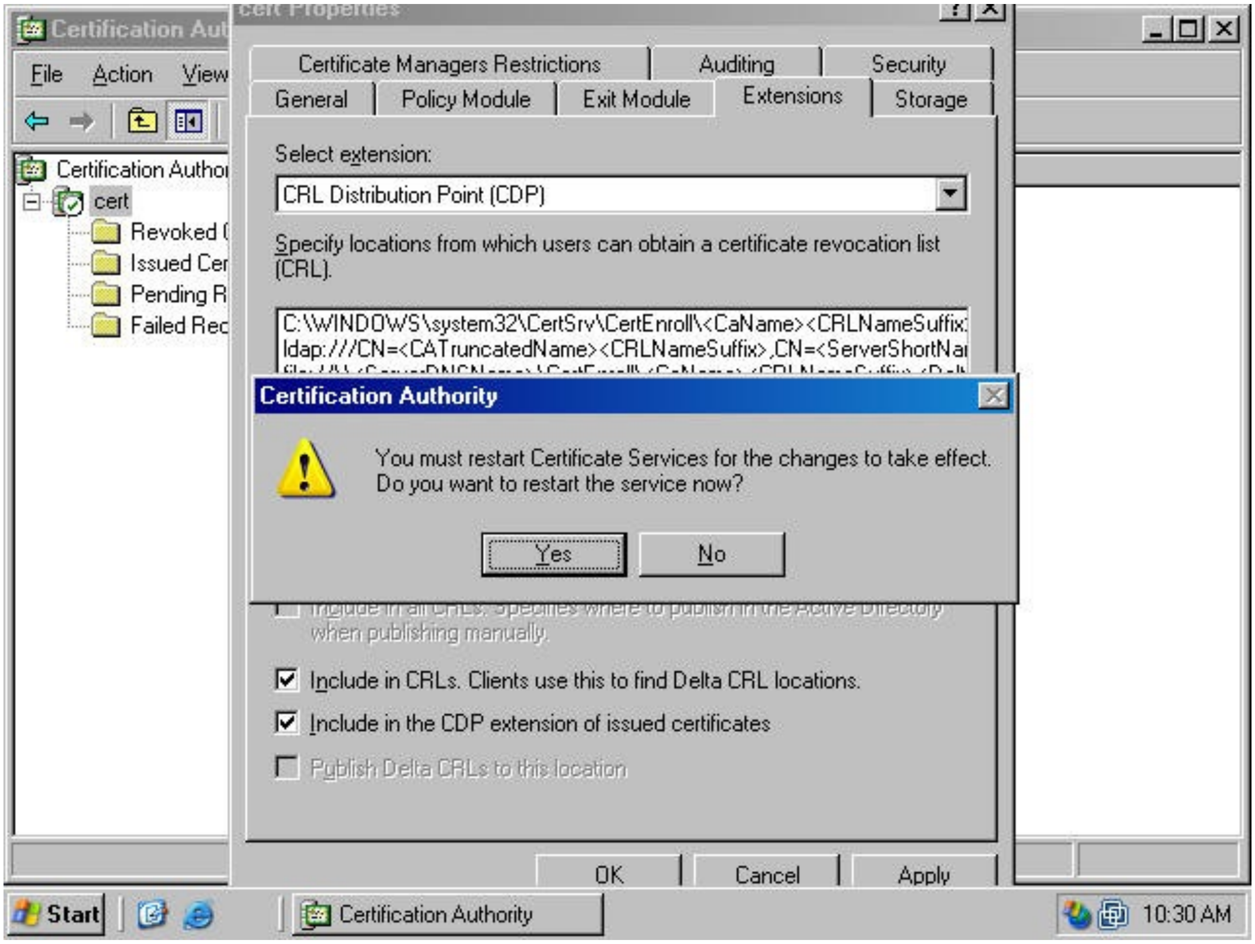
☑ Include in CRLs. Clients use this to find Delta CRL locations.

☑ Include in the CDP extension of issued certificates

☐ Publish Delta CRLs to this location

10. Click **Yes** in the **Certification Authority** dialog box (figure 31).

Figure 31



Select extension:

CRL Distribution Point (CDP)

Specify locations from which users can obtain a certificate revocation list (CRL).

C:\WINDOWS\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix:
ldap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortNa

Certification Authority

You must restart Certificate Services for the changes to take effect.
Do you want to restart the service now?

Yes No

☐ Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.

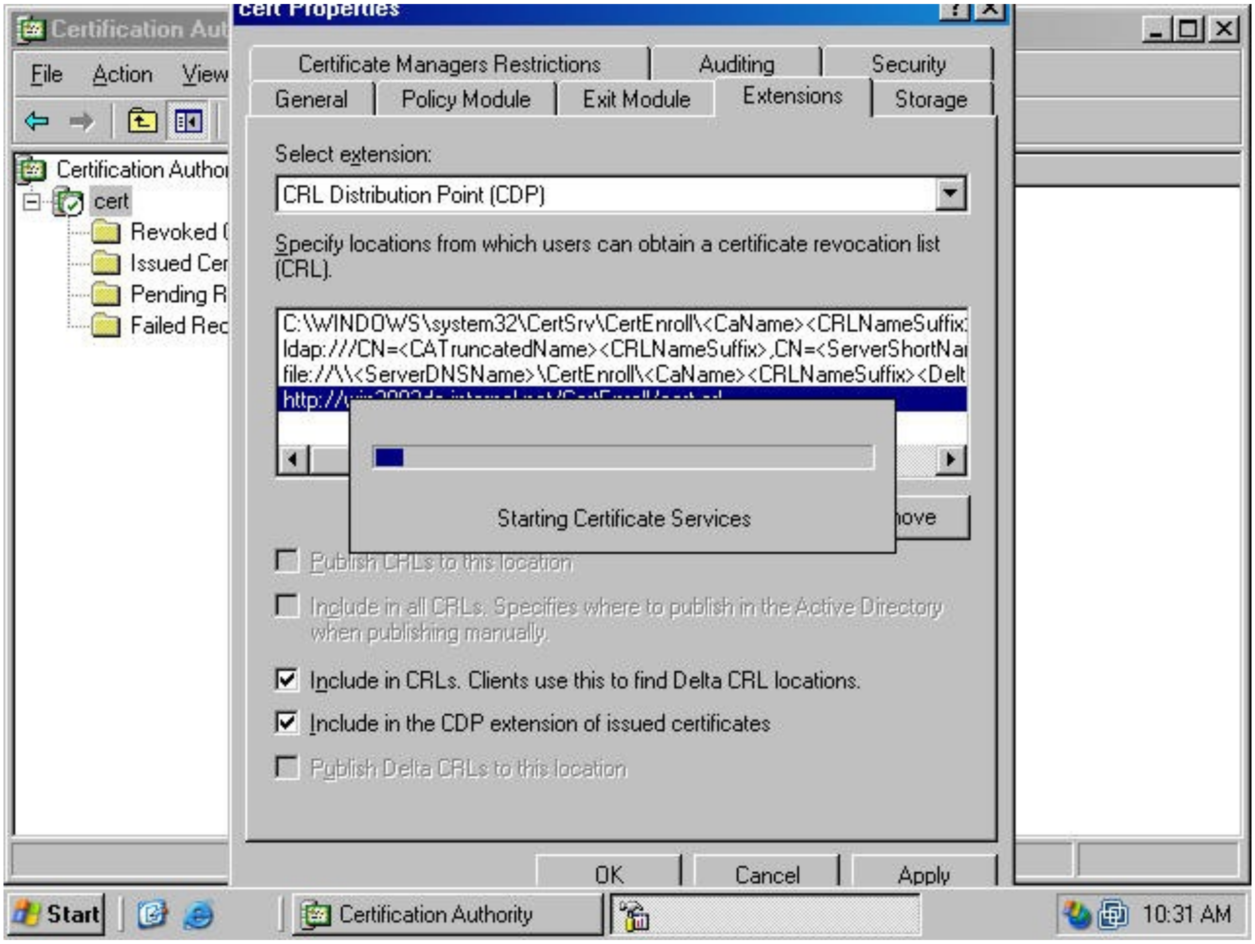
☑ Include in CRLs. Clients use this to find Delta CRL locations.

☑ Include in the CDP extension of issued certificates

☐ Publish Delta CRLs to this location

11. The Certificate Server service restarts (figure 32).

Figure 32



Select extension: CRL Distribution Point (CDP)

Specify locations from which users can obtain a certificate revocation list (CRL).

```
C:\WINDOWS\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix
ldap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortNa
file://\\<ServerDNSName>\CertEnroll\<CaName><CRLNameSuffix><Delt
http://
```

Starting Certificate Services

□ Publish CRLs to this location

□ Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.

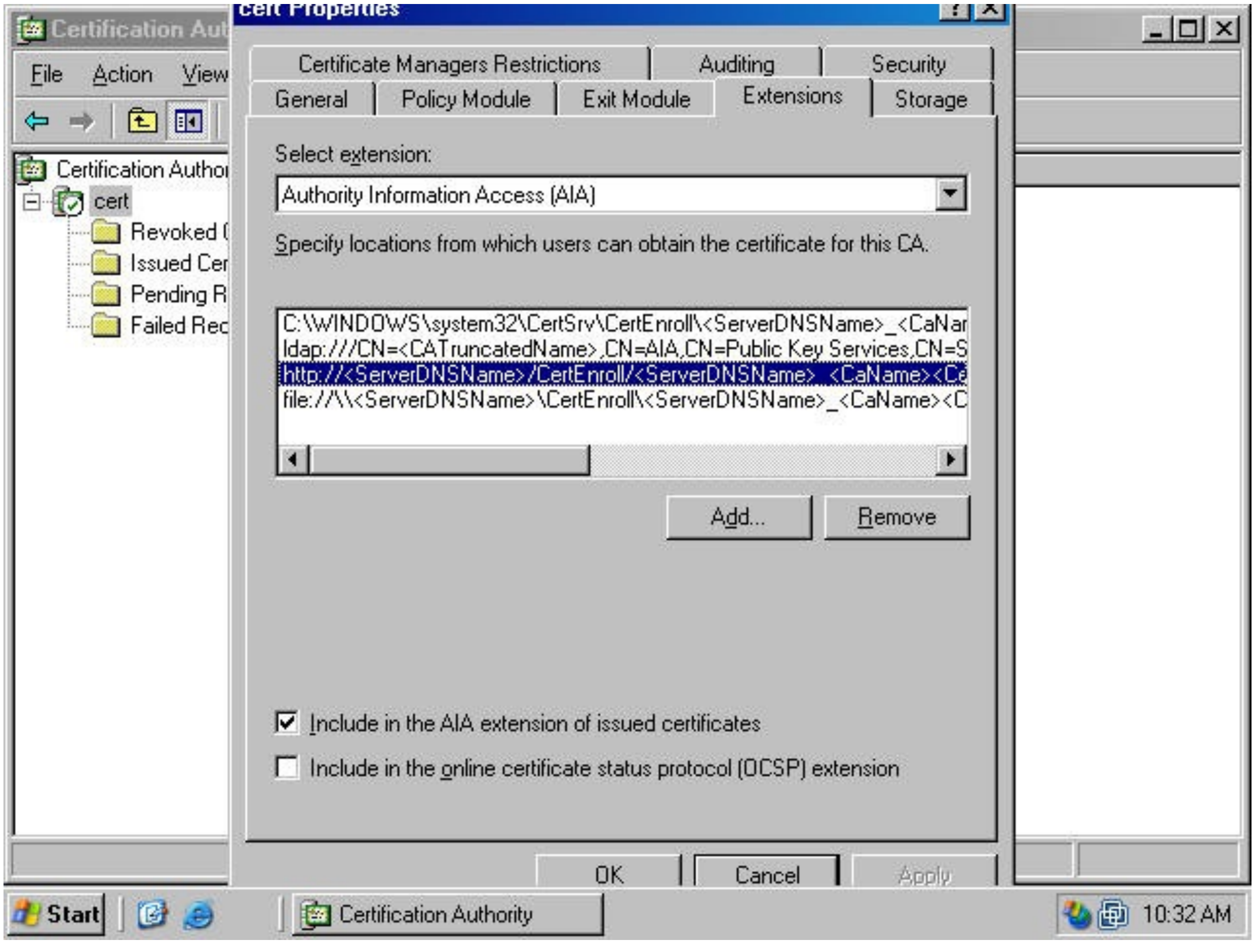
☑ Include in CRLs. Clients use this to find Delta CRL locations.

☑ Include in the CDP extension of issued certificates

□ Publish Delta CRLs to this location

12. Click the down arrow in the **Select extension** drop down list box and select the **Authority Information Access (AIA)** option. Select the location that begins with **http://** from the list of locations and click the **Remove** button (figure 33).

Figure 33



Select extension: Authority Information Access (AIA)

Specify locations from which users can obtain the certificate for this CA.

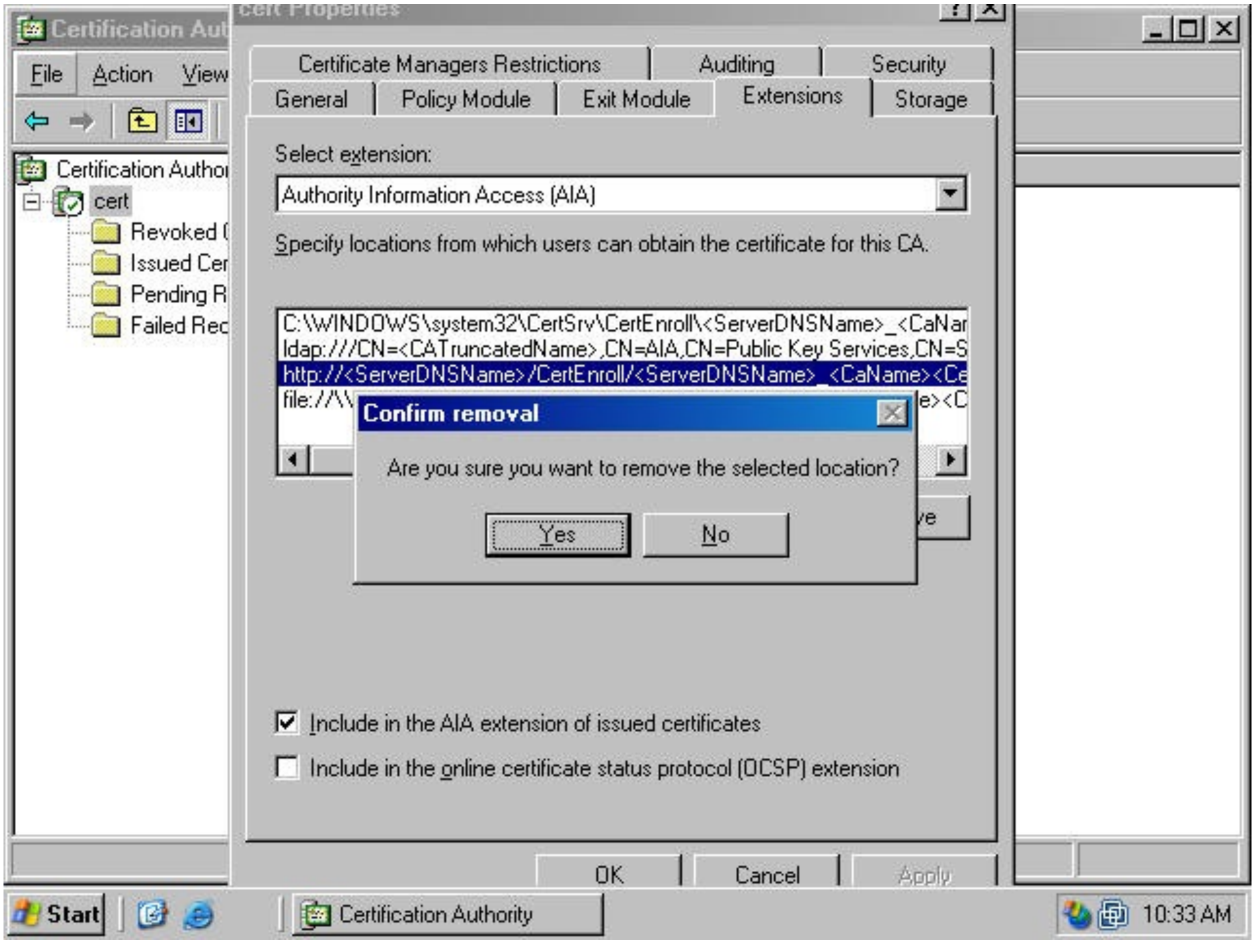
```
C:\WINDOWS\system32\CertSrv\CertEnroll\<ServerDNSName>_<CaNar
ldap:///CN=<CATruncatedName>,CN=AIA,CN=Public Key Services,CN=S
http://<ServerDNSName>/CertEnroll/<ServerDNSName>_<CaName><Ce
file://\\<ServerDNSName>\CertEnroll\<ServerDNSName>_<CaName><C
```

☑ Include in the AIA extension of issued certificates

□ Include in the online certificate status protocol (OCSP) extension

13. Click **Yes** in the **Confirm removal** dialog box (figure 34).

Figure 34



Select extension:

Authority Information Access (AIA)

Specify locations from which users can obtain the certificate for this CA.

```
C:\WINDOWS\system32\CertSrv\CertEnroll\<ServerDNSName>_<CaNar
ldap:///CN=<CATruncatedName>,CN=AIA,CN=Public Key Services,CN=S
http://<ServerDNSName>/CertEnroll/<ServerDNSName>_<CaName><Ce
file://\\                                                    e><C
```

Confirm removal

Are you sure you want to remove the selected location?

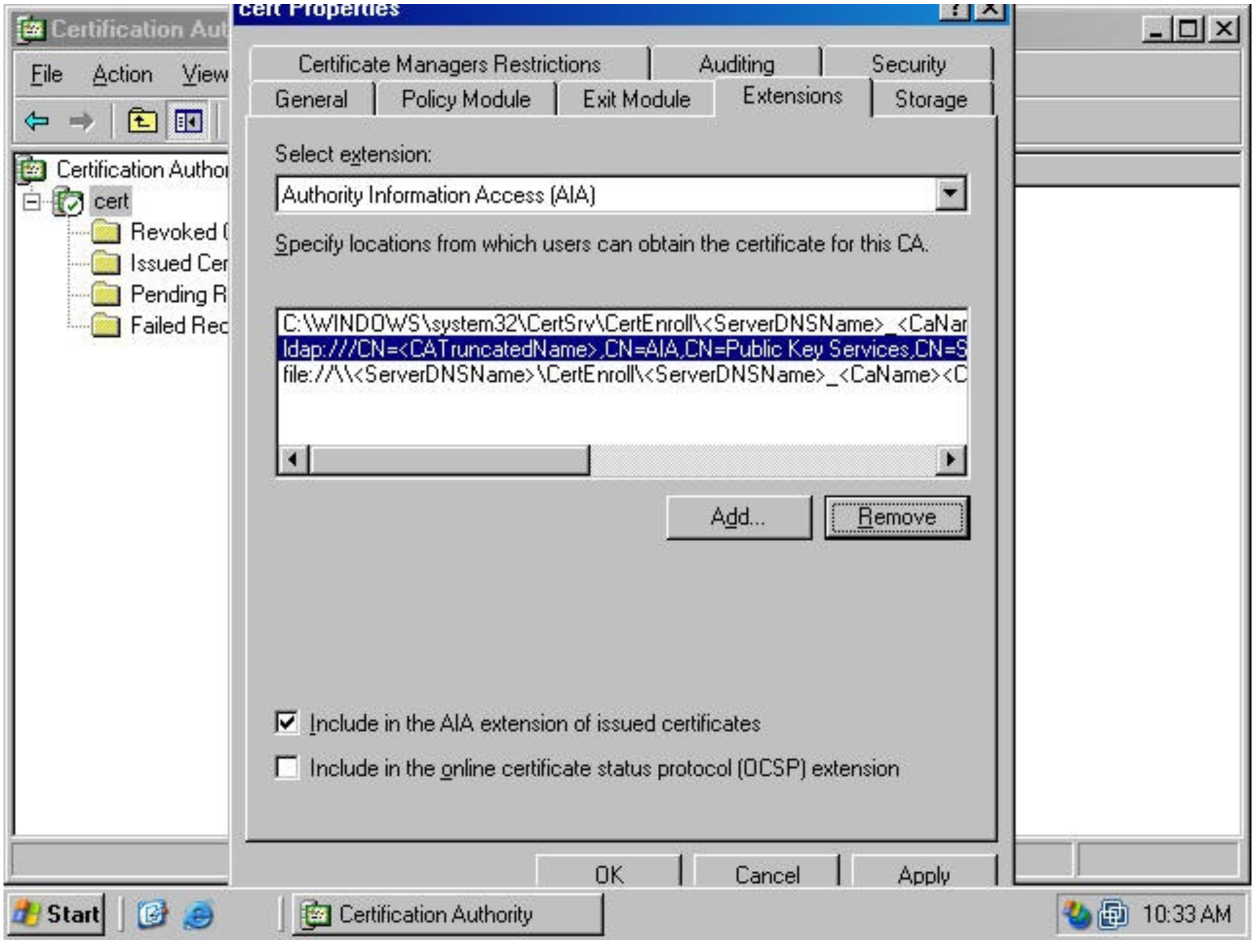
Yes No

☑ Include in the AIA extension of issued certificates

□ Include in the online certificate status protocol (OCSP) extension

14. Click the **Add** button on the **Extensions** tab (figure 35).

Figure 35



Select extension:

Authority Information Access (AIA)

Specify locations from which users can obtain the certificate for this CA.

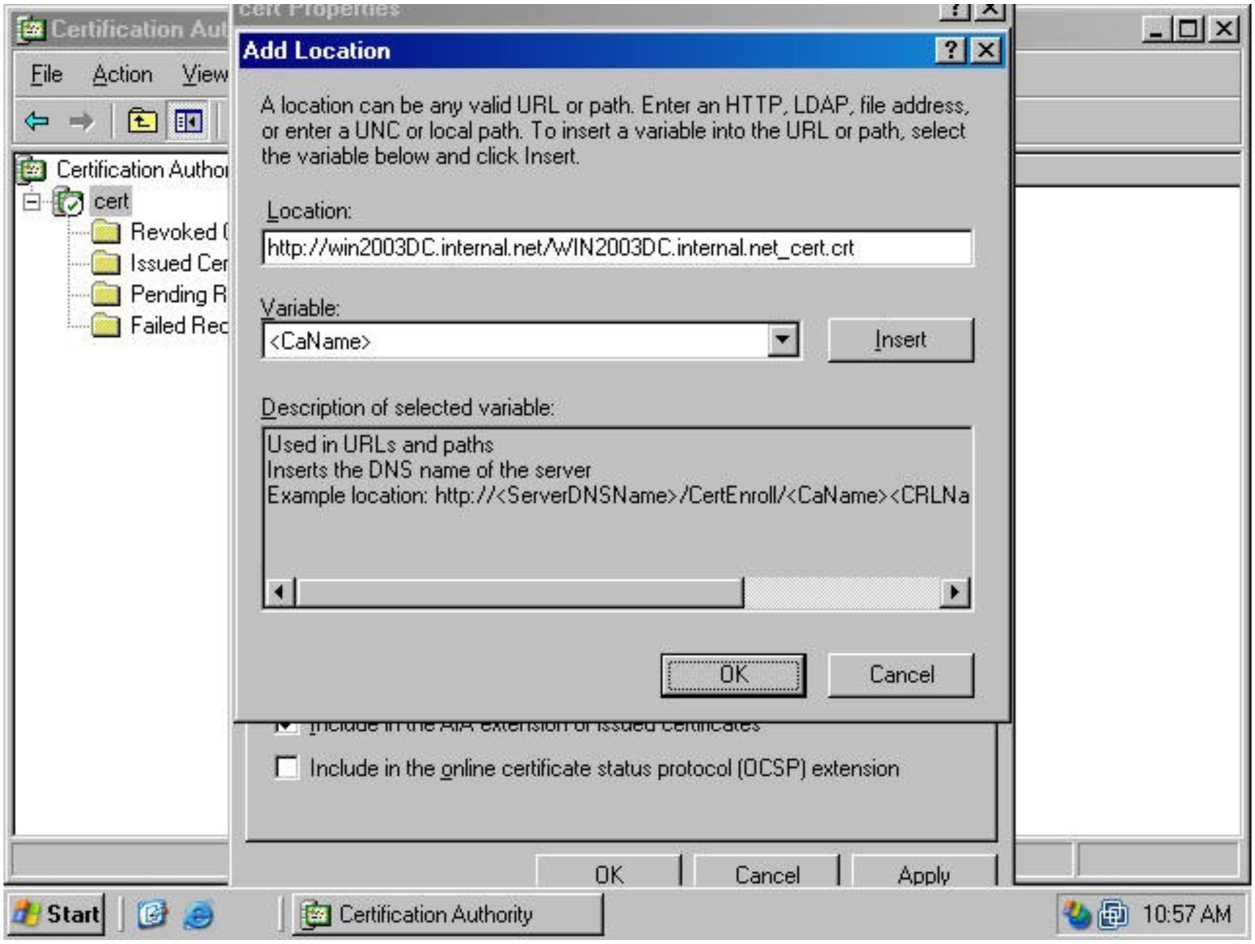
C:\WINDOWS\system32\CertSrv\CertEnroll\<ServerDNSName>_<CaNar
ldap:///CN=<CATruncatedName>,CN=AIA,CN=Public Key Services,CN=S
file://\\<ServerDNSName>\CertEnroll\<ServerDNSName>_<CaName><C

☑ Include in the AIA extension of issued certificates

☐ Include in the online certificate status protocol (OCSP) extension

15. In the **Add Location** dialog box, type the path to the Certificate Trust List in the **Location** text box. In this example, the path to the CTL is http://win2003dc.tacteam.net/WIN2003DC.internal.net_cert.crt. Click **OK** (figure 36).

Figure 36



A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.

Location:
http://win2003DC.internal.net/WIN2003DC.internal.net_cert.crt

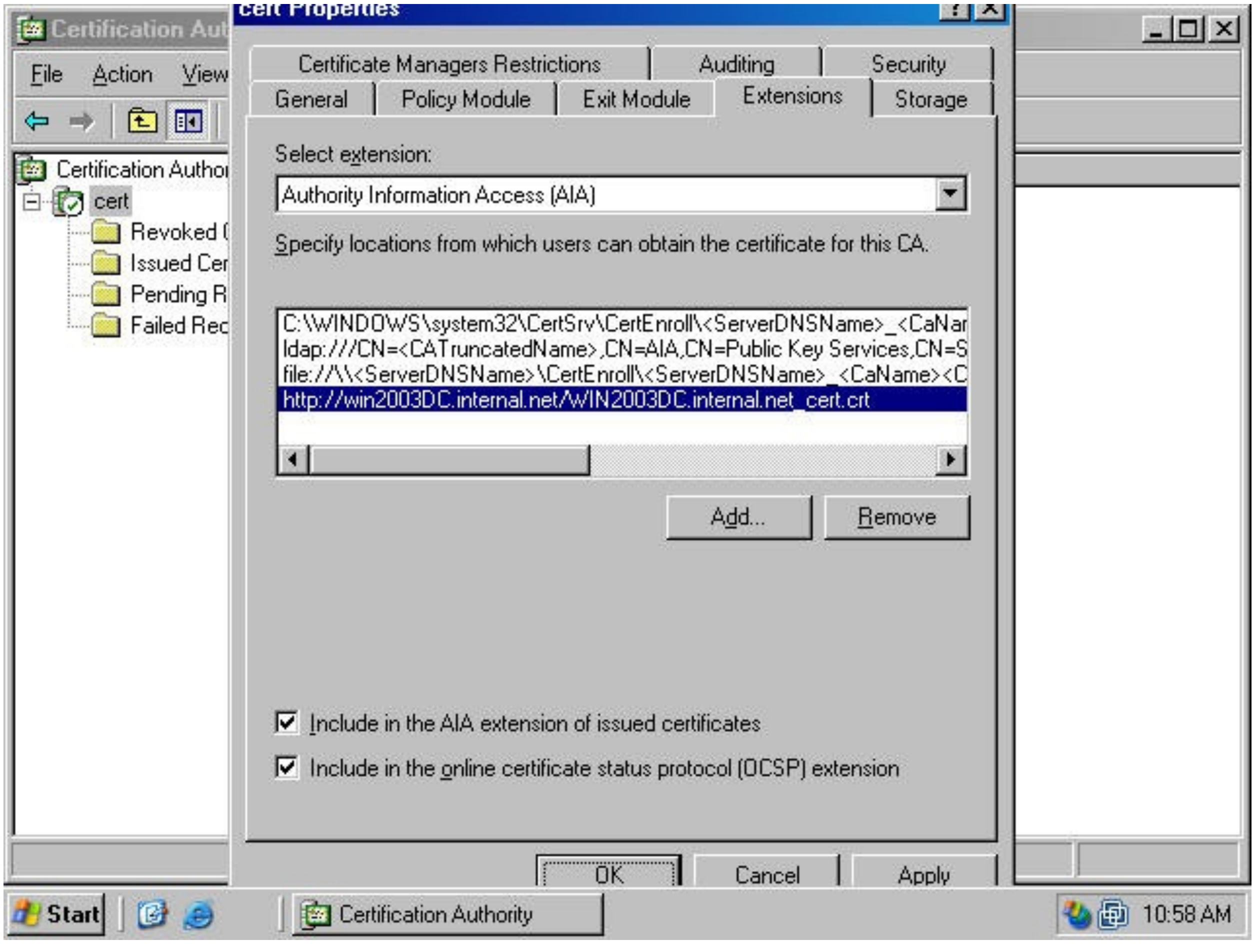
Variable:
<CaName>

Description of selected variable:
Used in URLs and paths
Inserts the DNS name of the server
Example location: http://<ServerDNSName>/CertEnroll/<CaName><CRLNa

☑ Include in the AIA extension of issued certificates
☐ Include in the online certificate status protocol (OCSP) extension

16. Place checkmarks in the **Include in the AIA extension of issued certificates** and **Include in the online certificate status protocol (OCSP) extension** checkboxes. Click **Apply** (figure 37).

Figure 37



Select extension:

Authority Information Access (AIA)

Specify locations from which users can obtain the certificate for this CA.

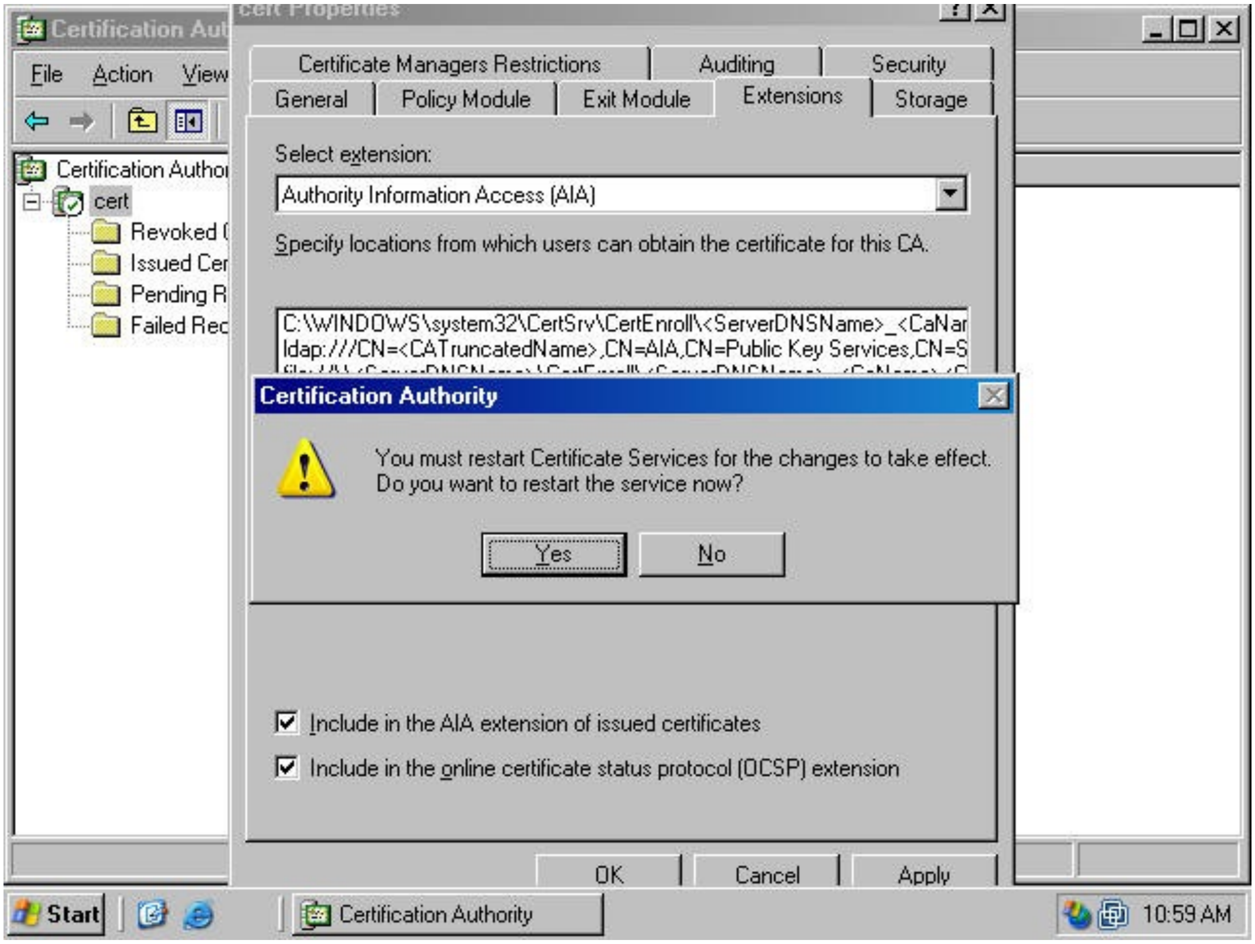
```
C:\WINDOWS\system32\CertSrv\CertEnroll\<ServerDNSName>_<CaNar
ldap:///CN=<CATruncatedName>,CN=AIA,CN=Public Key Services,CN=S
file://\\<ServerDNSName>\CertEnroll\<ServerDNSName>_<CaName><C
http://win2003DC.internal.net/WIN2003DC.internal.net_cert.crt
```

☑ Include in the AIA extension of issued certificates

☑ Include in the online certificate status protocol (OCSP) extension

17. Click **Yes** in the **Certification Authority** dialog box (figure 38).

Figure 38



Select extension:

Authority Information Access (AIA)

Specify locations from which users can obtain the certificate for this CA.

C:\WINDOWS\system32\CertSrv\CertEnroll\<ServerDNSName>_<CaNar
ldap:///CN=<CATruncatedName>,CN=AIA,CN=Public Key Services,CN=S

Certification Authority

You must restart Certificate Services for the changes to take effect. Do you want to restart the service now?

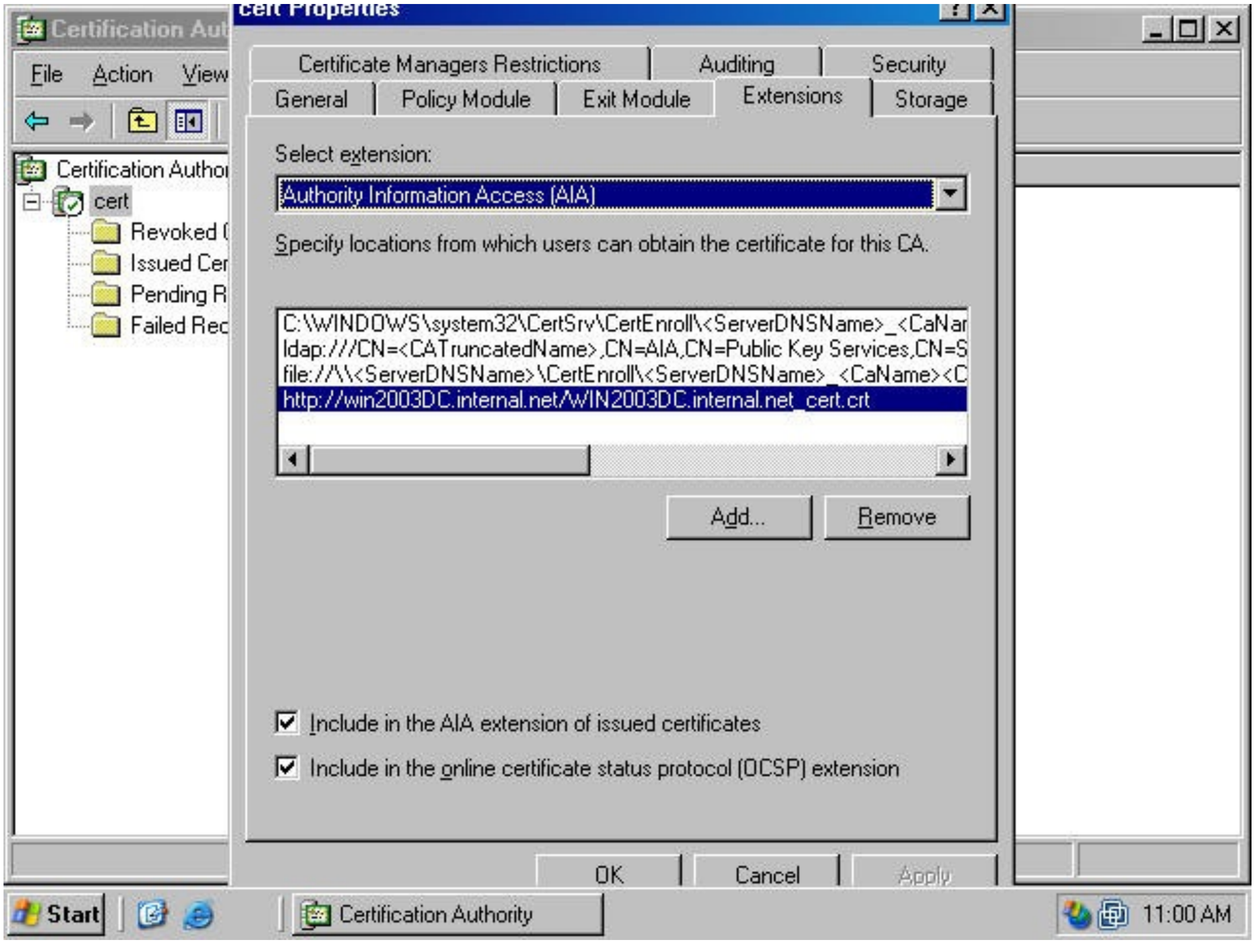
Yes No

☑ Include in the AIA extension of issued certificates

☑ Include in the online certificate status protocol (OCSP) extension

18. Click **OK** on the server **Properties** dialog box (figure 39).

Figure 39



Select extension:

Authority Information Access (AIA)

Specify locations from which users can obtain the certificate for this CA.

```
C:\WINDOWS\system32\CertSrv\CertEnroll\<ServerDNSName>_<CaNar
ldap:///CN=<CATruncatedName>,CN=AIA,CN=Public Key Services,CN=S
file://\\<ServerDNSName>\CertEnroll\<ServerDNSName>_<CaName><C
http://win2003DC.internal.net/WIN2003DC.internal.net_cert.crt
```

☑ Include in the AIA extension of issued certificates

☑ Include in the online certificate status protocol (OCSP) extension

Create a DNS Entry in the Public DNS for the Published CA

There must be a public DNS entry for the Fully Qualified Domain Name listed in the CRL. The external network client must be able to resolve the FQDN found in the CRL to the IP address on external interface address on the ISA firewall/VPN server that is being used for the Incoming Web Requests listener.

For example, if the public address used by the Incoming Web Requests listener is **131.107.0.1** and the FQDN in the CRL is **cert.internal.net**, then you must create a Host (A) resource record in the public DNS that resolves **cert.internal.net** to 131.107.0.1.

If your ISP hosts your public DNS records, you can ask your ISP to make the change or if your ISP allows you to manipulate your own DNS records, you can use their administrative interface to make the changes. If you publish your own DNS servers, you can add the record on your own published DNS servers.

Note that you can only provide a single HTTP location that users can use to obtain a certificate. You cannot provide an internal network FQDN location and a separate external network FQDN location. While you can create multiple HTTP locations, only the location at the top of the list will be used if it is available. Alternate locations are queried only when the those higher on the list are not available. You should create a split DNS infrastructure to support internal external network clients name resolution for the CRL locations.

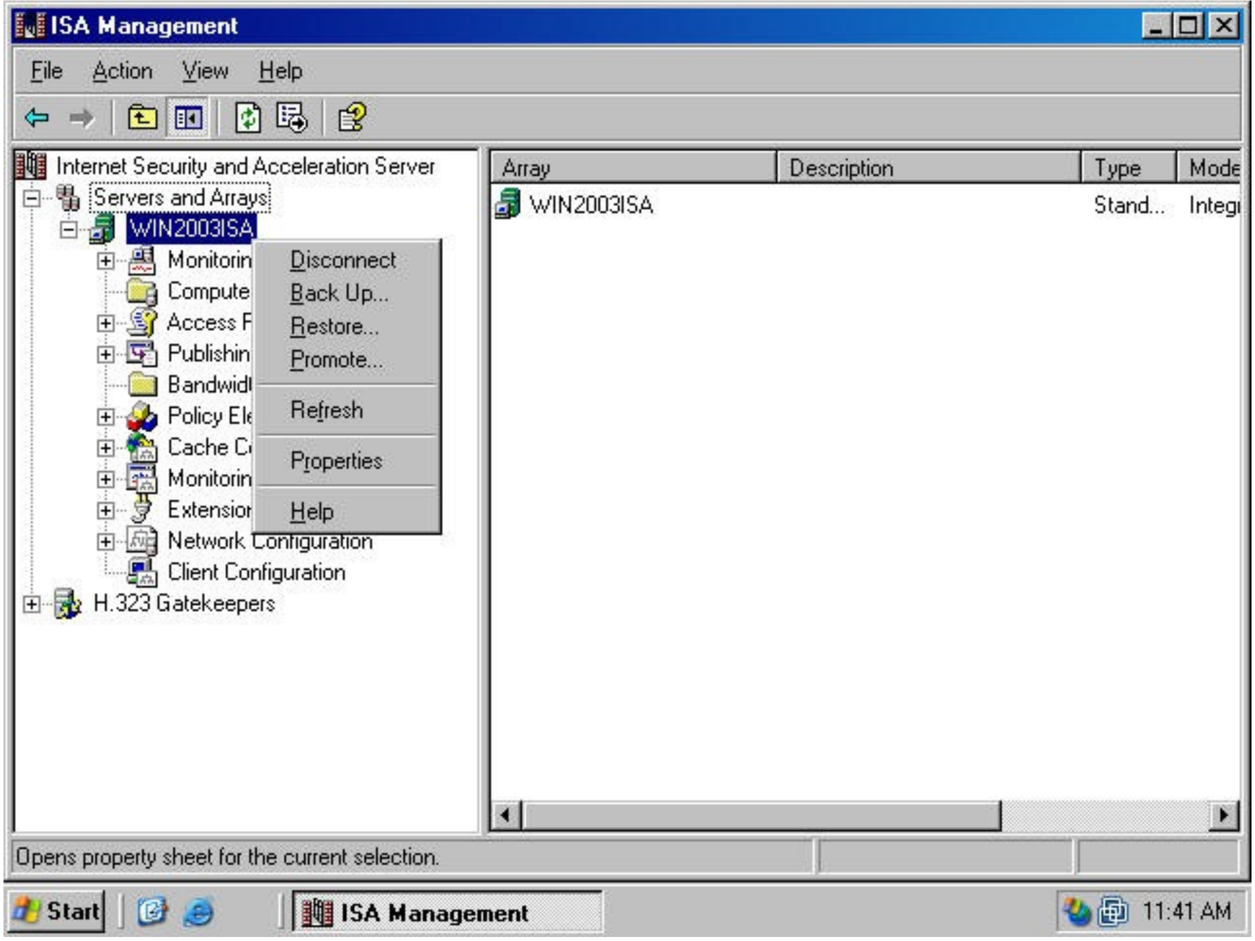
Configure the Incoming Web Requests Listener

The Incoming Web Requests listener accepts requests for the published Web server. The listener accepts the request from the external client and sends the request to the Web Proxy service for evaluation. If the request matches the settings in a Web Publishing Rule, the request is forwarded to the published server. If there is no matching Web Publishing Rule, the request is dropped.

Perform the following steps to configure the Incoming Web Requests listener on the ISA firewall:

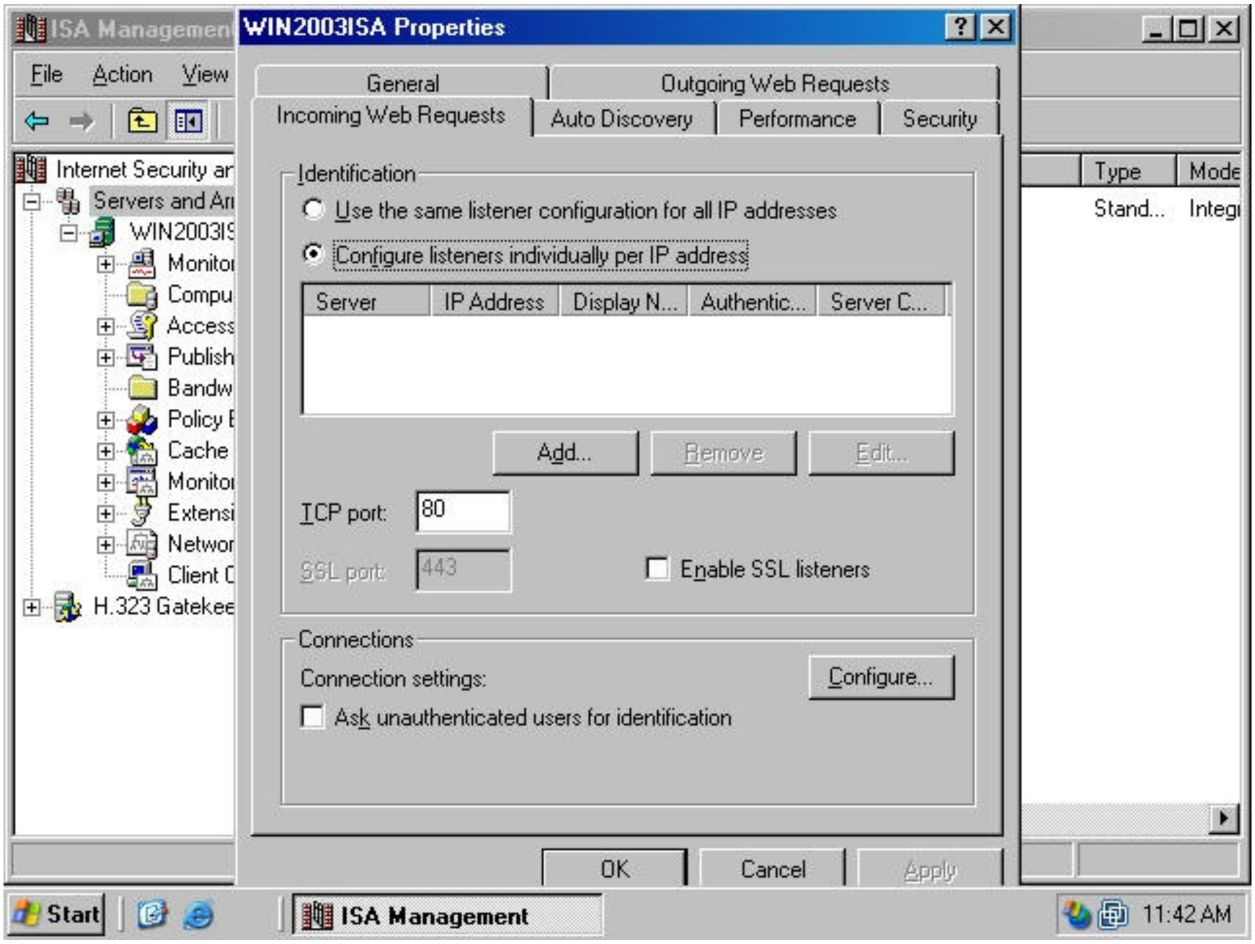
1. Open the **ISA Management** console, expand the **Servers and Arrays** node and then expand your server name. Right click on your server name and click the **Properties** command (figure 40).

Figure 40



2. In the server **Properties** dialog box, click the **Incoming Web Requests** tab (figure 41). On the **Incoming Requests** tab, select the **Configure listeners individually per IP address** option, then click the **Add** button to configure the listener.

Figure 41



Identification

○ Use the same listener configuration for all IP addresses

● Configure listeners individually per IP address

Server	IP Address	Display N...	Authentic...	Server C...

TCP port: 80

SSL port: 443

□ Enable SSL listeners

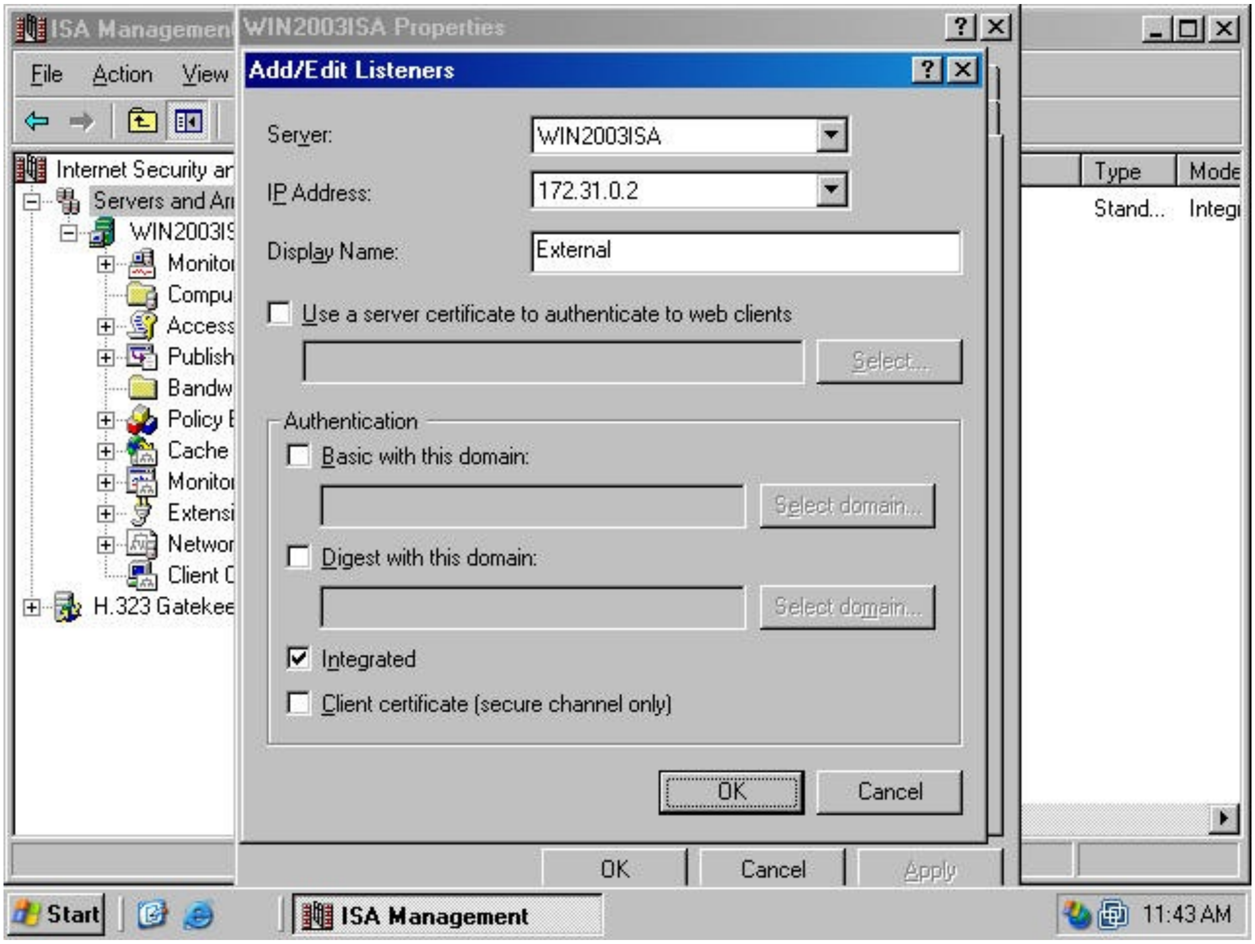
Connections

Connection settings:

□ Ask unauthenticated users for identification

3. On the **Add/Edit Listeners** dialog box, use the drop-down list boxes to select the **Server** you are working on, the **IP address** on the external interface you want the listener to listen on, and a **Display Name** that describes the listener. You will not use authentication at the listener when publishing the Web enrollment site, so you do not need to change the authentication settings (figure 42). Click **OK**.

Figure 42 (fig303)



Add/Edit Listeners

Server: WIN2003ISA

IP Address: 172.31.0.2

Display Name: External

□ Use a server certificate to authenticate to web clients

Authentication

□ Basic with this domain:

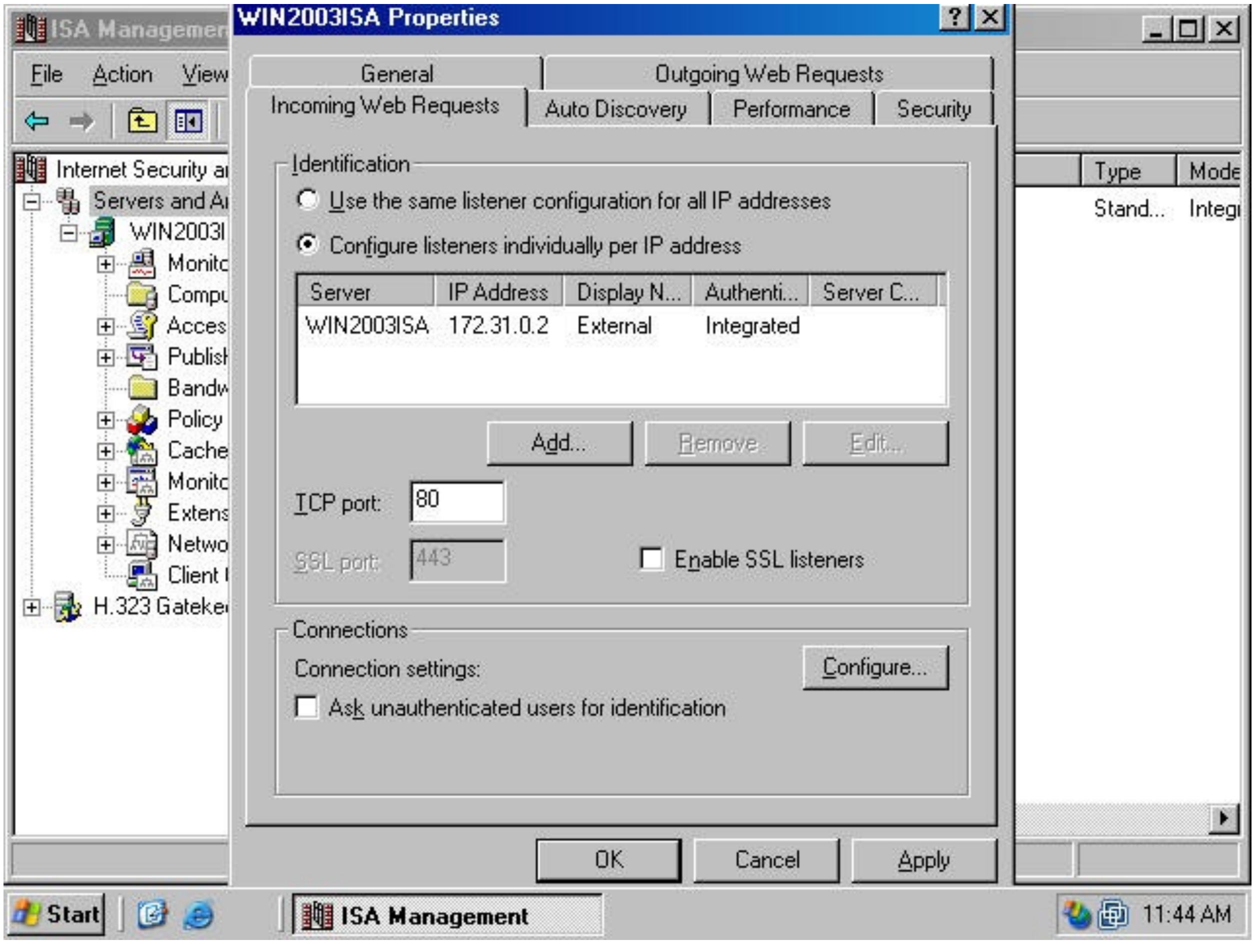
□ Digest with this domain:

☑ Integrated

□ Client certificate (secure channel only)

4. Click **Apply** on the server **Properties** dialog box (figure 43)

Figure 43



○ Use the same listener configuration for all IP addresses

● Configure listeners individually per IP address

Server	IP Address	Display N...	Authenti...	Server C...
WIN2003ISA	172.31.0.2	External	Integrated	

TCP port: 80

SSL port: 443

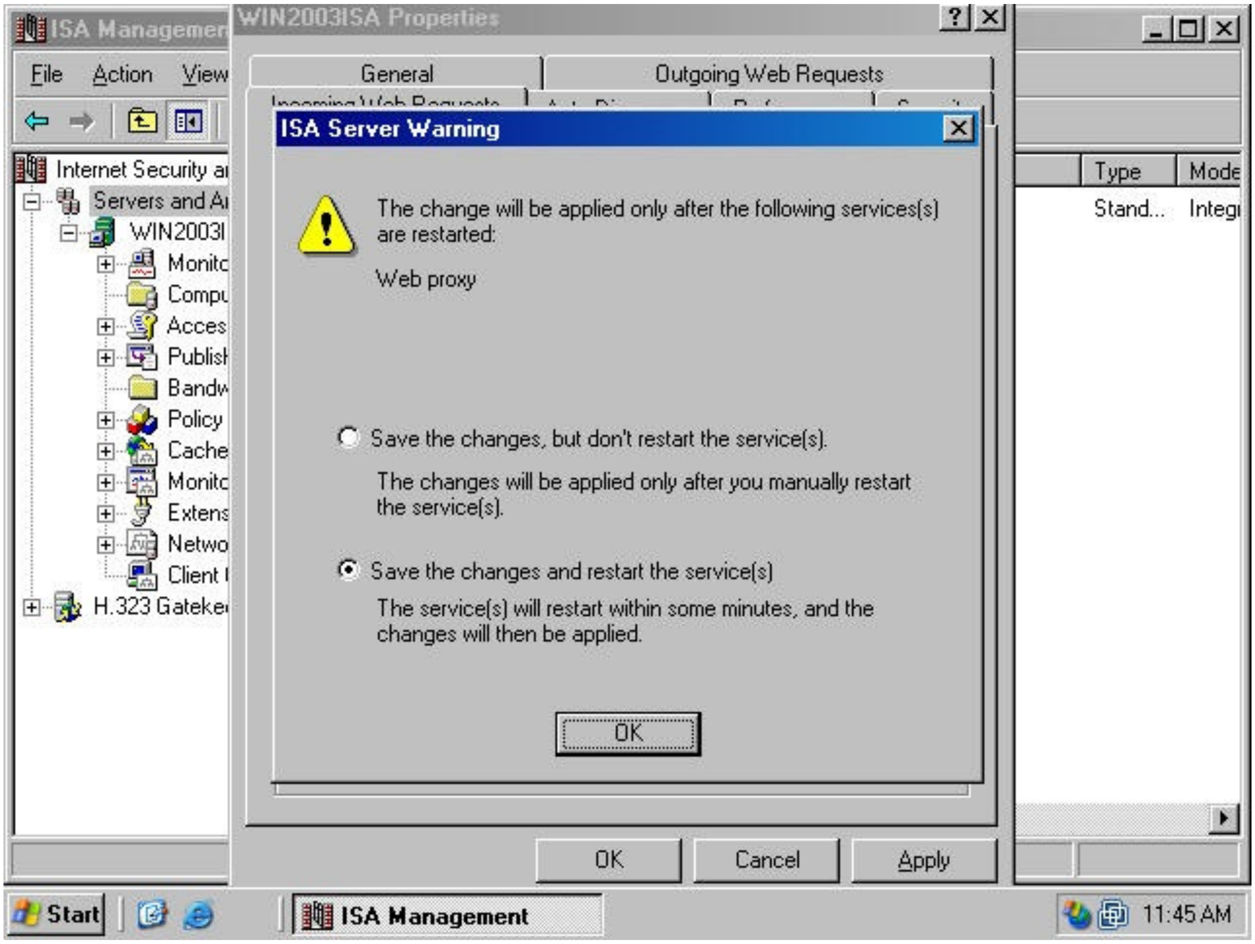
□ Enable SSL listeners

Connection settings: Configure...

□ Ask unauthenticated users for identification

5. In the **ISA Server Warning** dialog box, select the **Save the changes and restart the service(s)** option. This will cause the **Web proxy** service to restart and disconnect any users that are currently connected to the Web Proxy service. The users will automatically reconnect when the Web Proxy service restarts (figure 44).

Figure 44



ISA Server Warning

The change will be applied only after the following services(s) are restarted:

Web proxy

○ Save the changes, but don't restart the service(s).

The changes will be applied only after you manually restart the service(s).

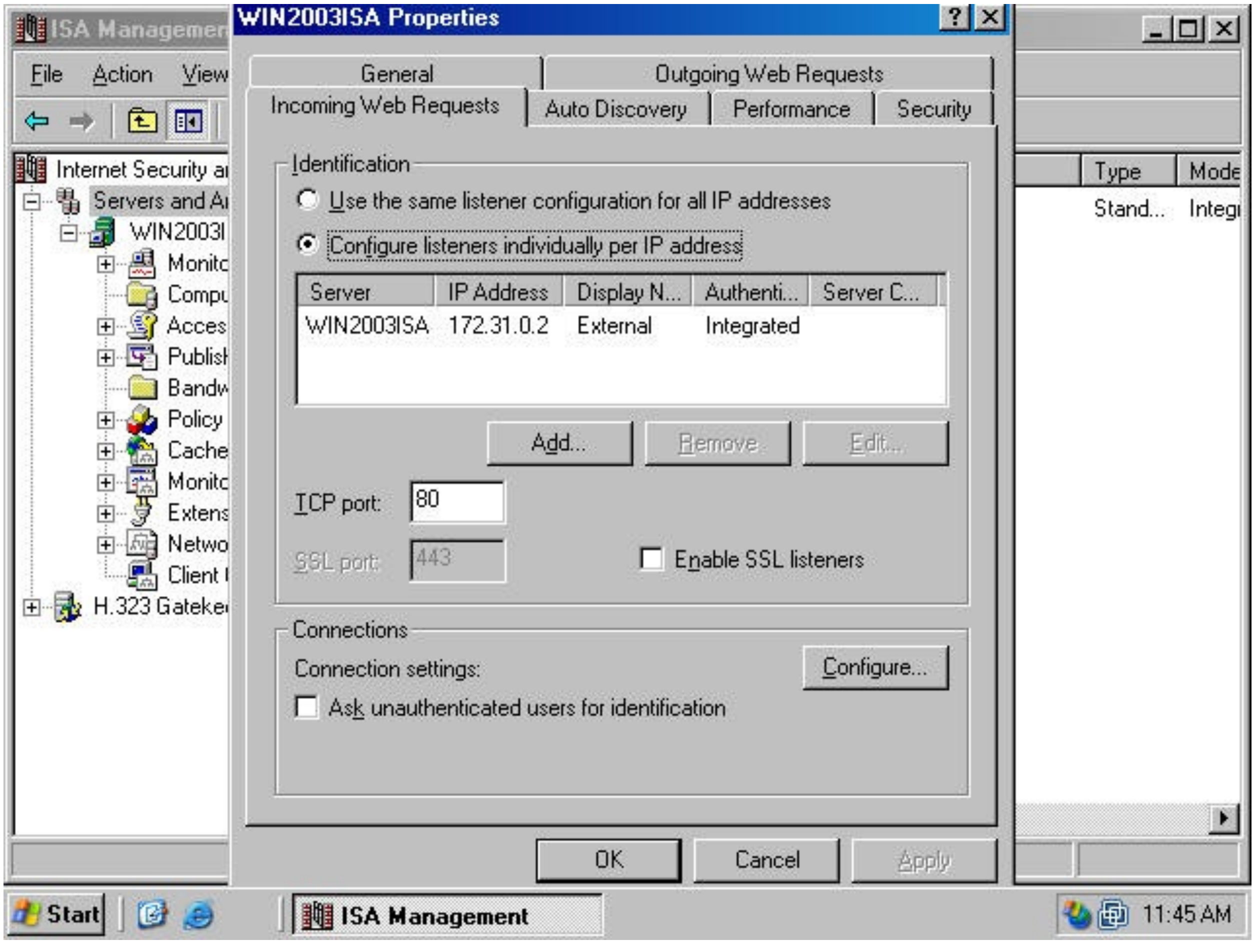
● Save the changes and restart the service(s)

The service(s) will restart within some minutes, and the changes will then be applied.

OK

6. Click **OK** in the server **Properties** dialog box (figure 45).

Figure 45



WIN2003ISA Properties

Identification

○ Use the same listener configuration for all IP addresses

● Configure listeners individually per IP address

Server	IP Address	Display N...	Authenti...	Server C...
WIN2003ISA	172.31.0.2	External	Integrated	

TCP port: 80

SSL port: 443

☐ Enable SSL listeners

Connections

Connection settings:

☐ Ask unauthenticated users for identification

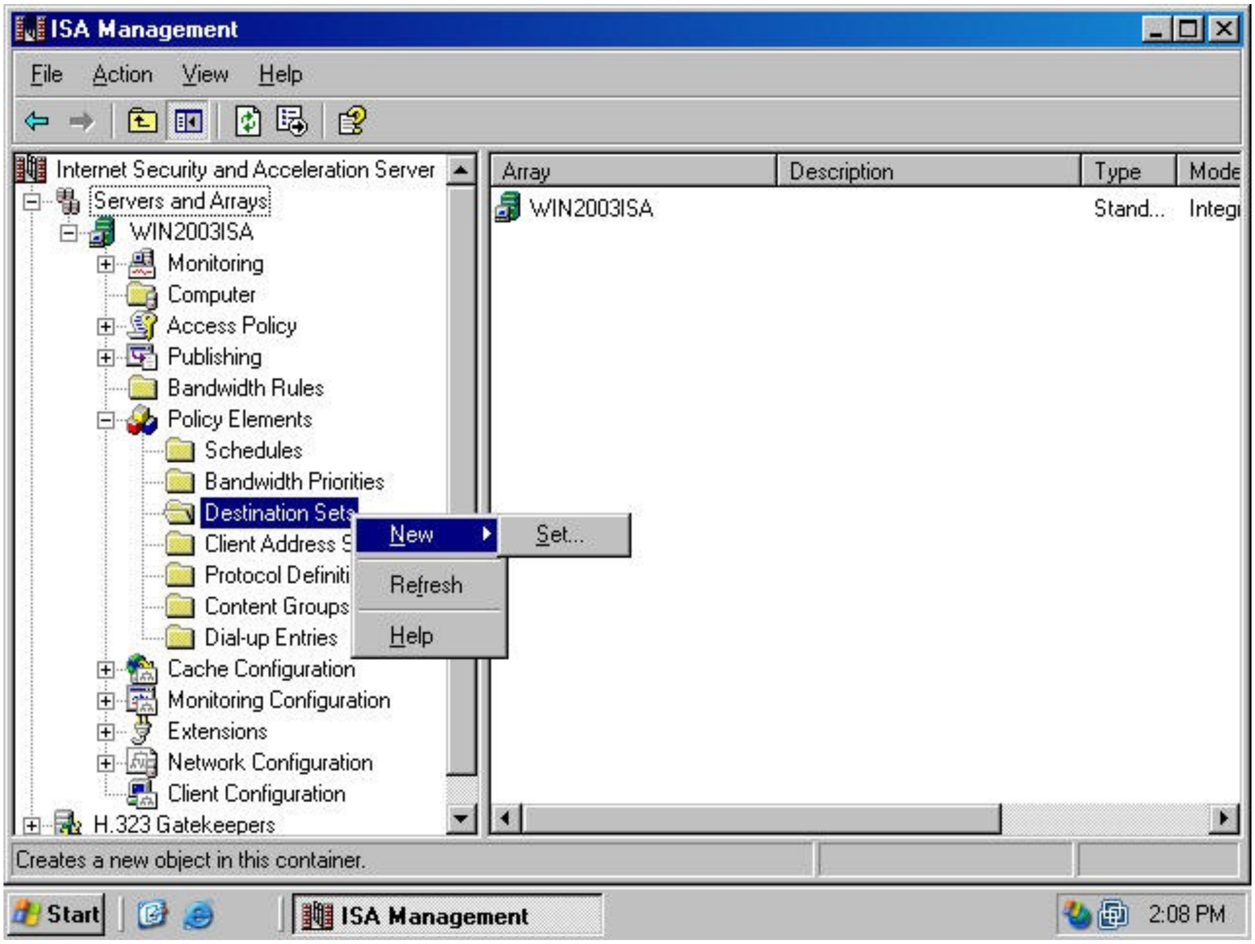
Create the Destination Set and HOSTS File Entry to Support the Web Publishing Rule

The Web Publishing Rule uses a Destination Set to match against the Host Header in the incoming request. For example, when the external user sends a request for http://www.internal.net, then the host header will contain the entry for www.internal.net. If the Web Publishing Rule contains a Destination Set that instructs it to listen for incoming connections to www.internal.net, then the Rule will further evaluate the request.

Perform the following steps to create the Destination Set you will use in the Web Publishing Rule:

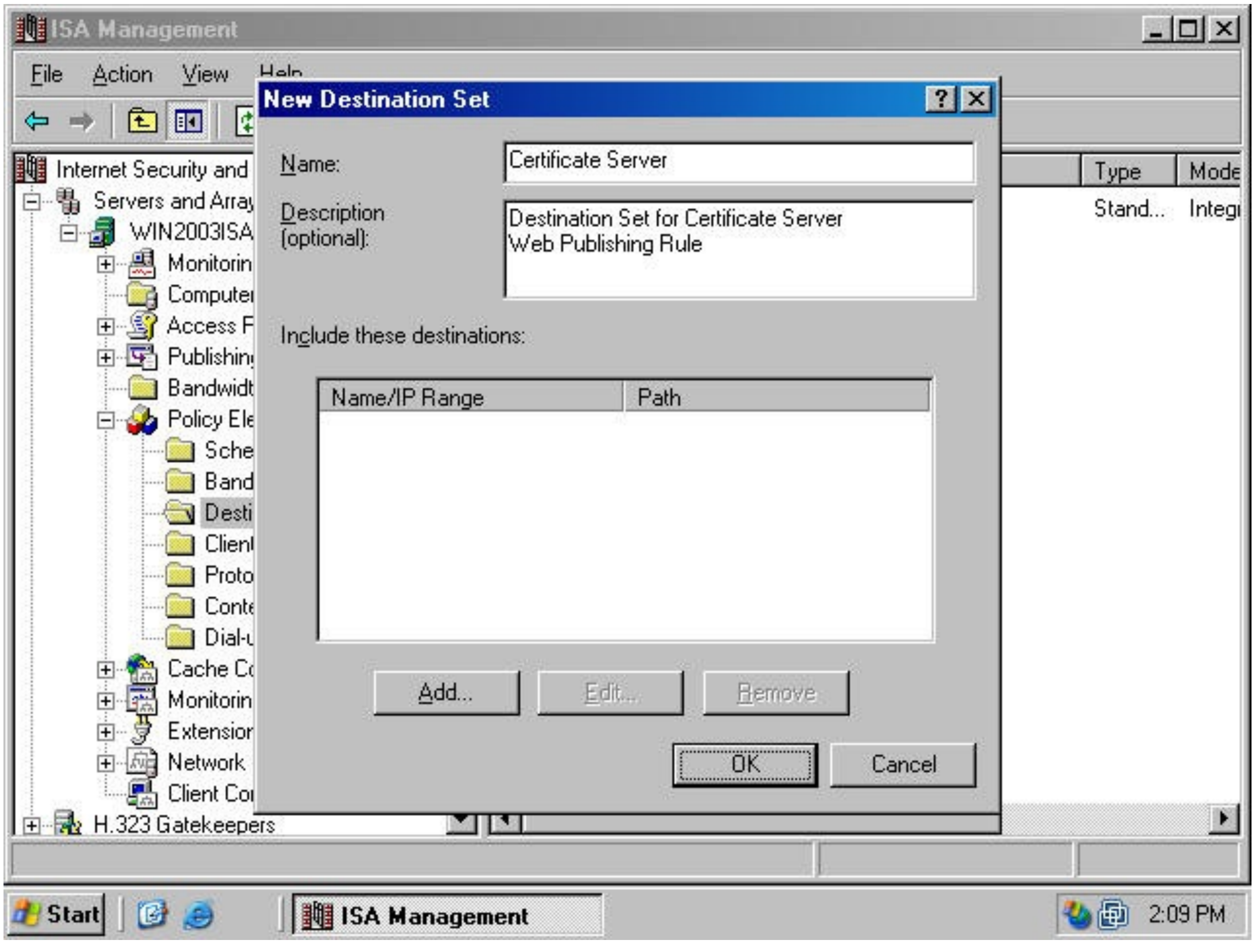
1. In the **ISA Management** console, expand the **Servers and Arrays** node and then expand the server node. Expand the **Policy Elements** node and right click on **Destination Sets**. Point to **New** and click on **Set** (figure 46).

Figure 46



2. In the **New Destination Set** dialog box, type in a name for the Destination Set. In this example we'll name the Destination Set **Certificate Server**. You can type in an optional description for the Destination Set. In this example we'll describe the Destination Set as **Destination Set for Certificate Server Web Publishing Rule**. Click the **Add** button in the **New Destination Set** dialog box (figure 47).

Figure 47



New Destination Set

Name: Certificate Server

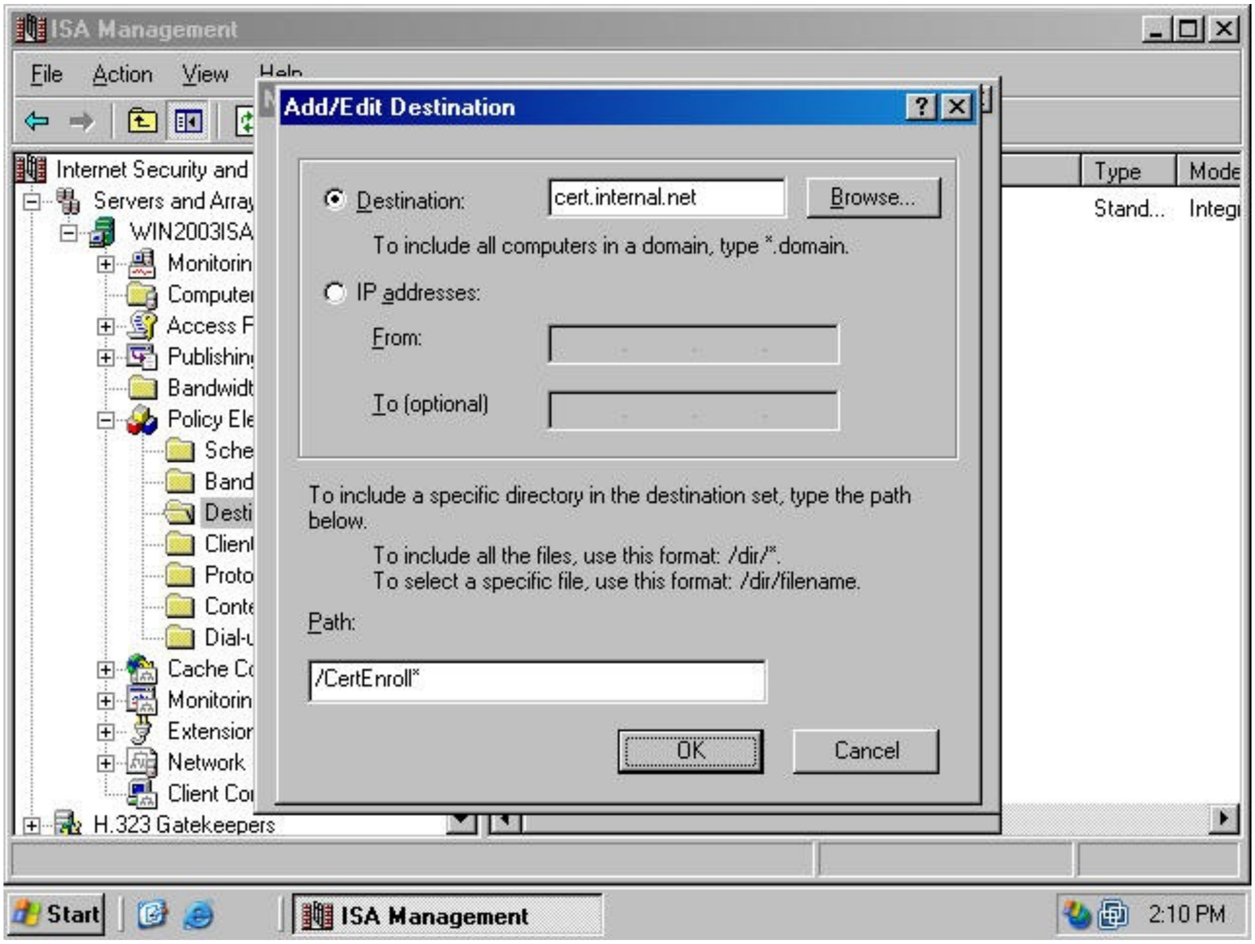
Description (optional): Destination Set for Certificate Server Web Publishing Rule

Include these destinations:

Name/IP Range	Path

3. In the **Add/Edit** dialog box, select the **Destination** option and type in the FQDN that the *external* user will use to access the certificate server Web enrollment site. In this example the external user will use the name **cert.internal.net**. Three paths are required: /**CertEnroll*** , /**CertControl*** and **/CertSrv***. Type **/CertEnroll*** in the **Path** text box and click **OK** (figure 48).

Figure 48



● Destination: cert.internal.net

To include all computers in a domain, type *.domain.

○ IP addresses:

From:

To (optional):

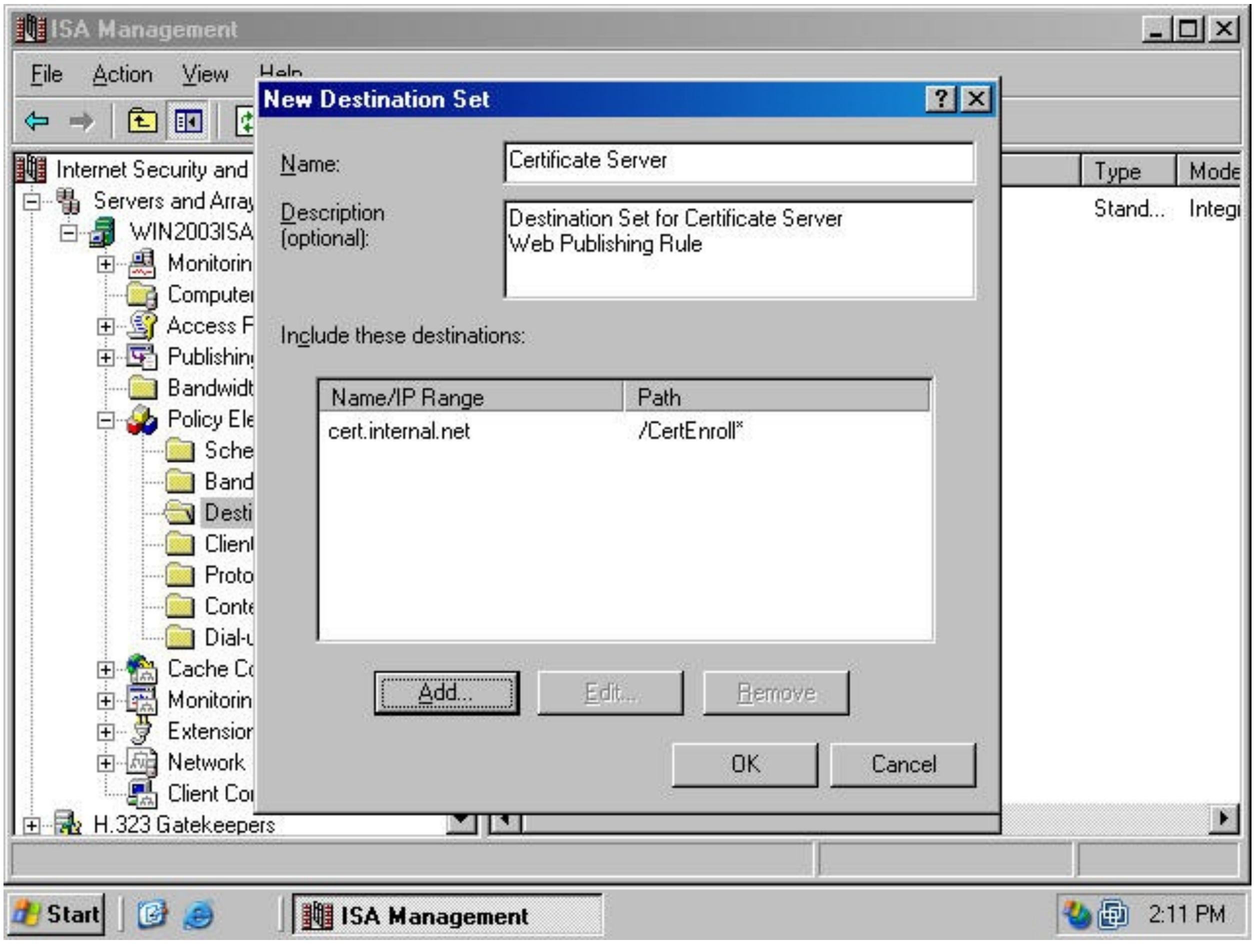
To include a specific directory in the destination set, type the path below.

To include all the files, use this format: /dir/*.
To select a specific file, use this format: /dir/filename.

Path: /CertEnroll*

4. Click the **Add** button in the **New Destination Set** dialog box (figure 49).

Figure 49



Name: Certificate Server

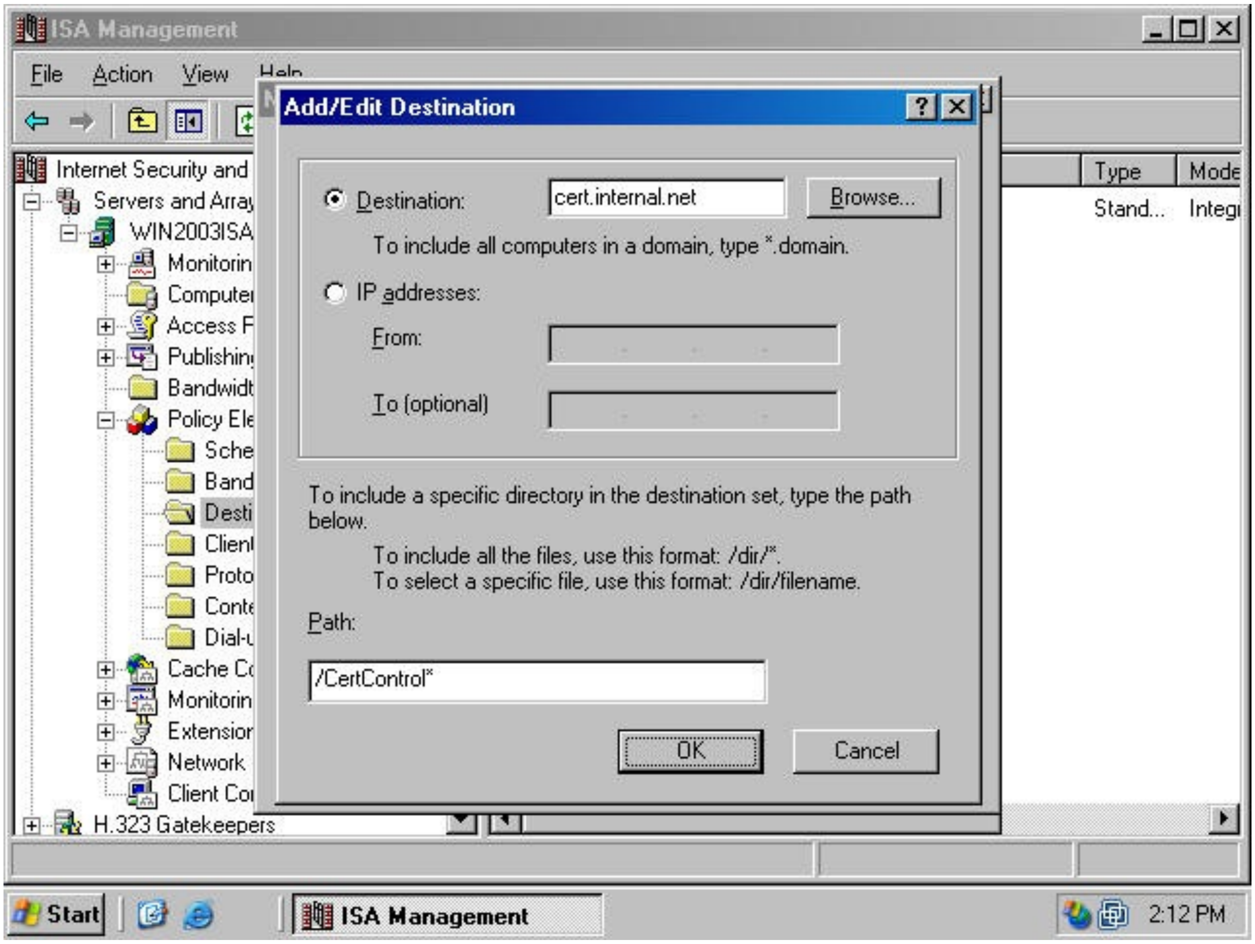
Description (optional): Destination Set for Certificate Server Web Publishing Rule

Include these destinations:

Name/IP Range	Path
cert.internal.net	/CertEnroll*

5. Select the **Destination** option and type in the FQDN used by the external user to access the Web enrollment site. Type **/CertControl*** in the **Path** text box (figure 50). Click **OK**.

Figure 50



● Destination: cert.internal.net

To include all computers in a domain, type *.domain.

○ IP addresses:

From:

To (optional)

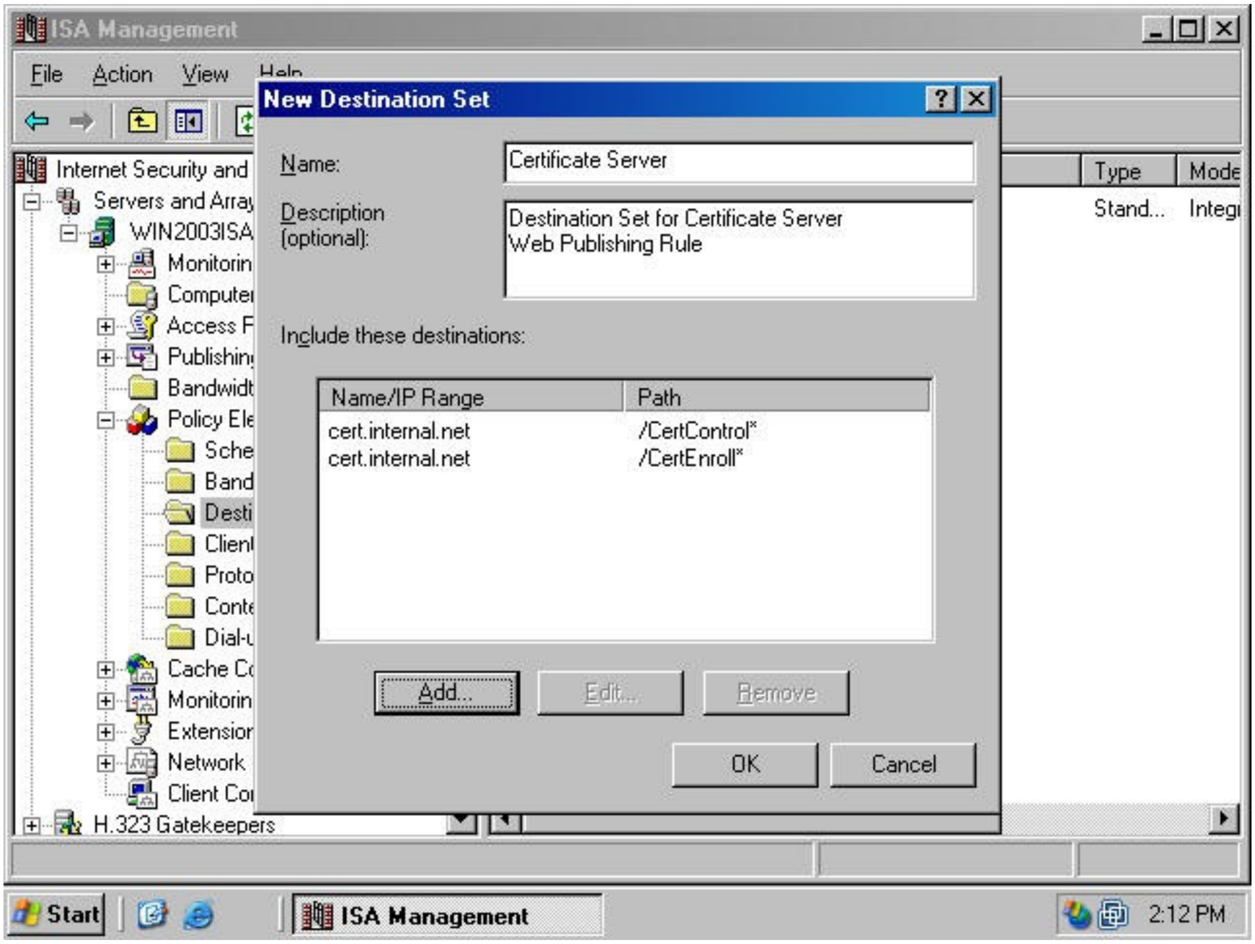
To include a specific directory in the destination set, type the path below.

To include all the files, use this format: /dir/*.
To select a specific file, use this format: /dir/filename.

Path: /CertControl*

6. Click the **Add** button in the **New Destination Set** dialog box (figure 51).

Figure 51



New Destination Set

Name: Certificate Server

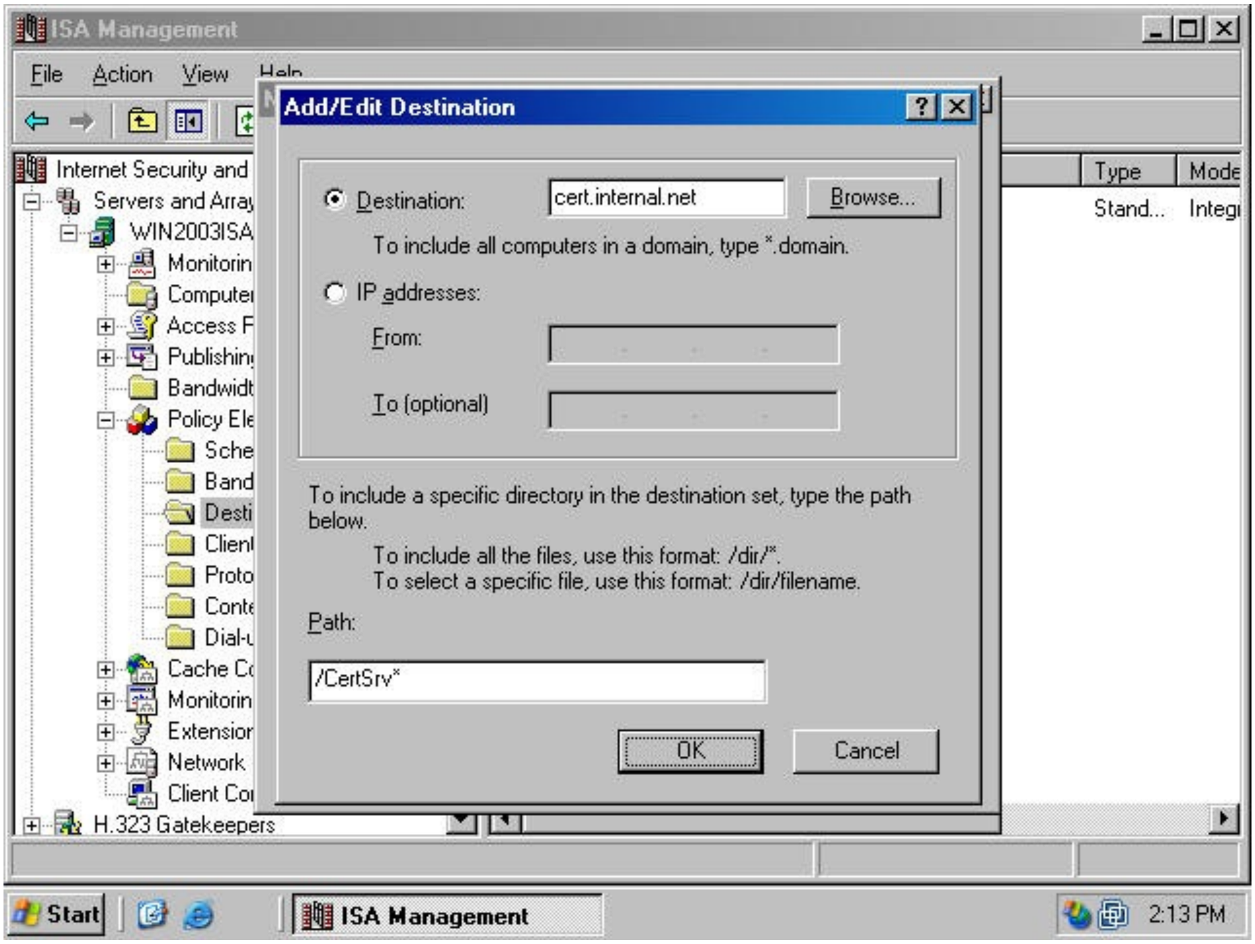
Description (optional): Destination Set for Certificate Server Web Publishing Rule

Include these destinations:

Name/IP Range	Path
cert.internal.net	/CertControl*
cert.internal.net	/CertEnroll*

7. Select the **Destination** option and type in the FQDN used by the external user to access the Web enrollment site. Type **/CertSrv*** in the **Path** text box (figure 52). Click **OK**.

Figure 52



Add/Edit Destination

● Destination: cert.internal.net

To include all computers in a domain, type *.domain.

○ IP addresses:

From:

To (optional)

To include a specific directory in the destination set, type the path below.

To include all the files, use this format: /dir/*.

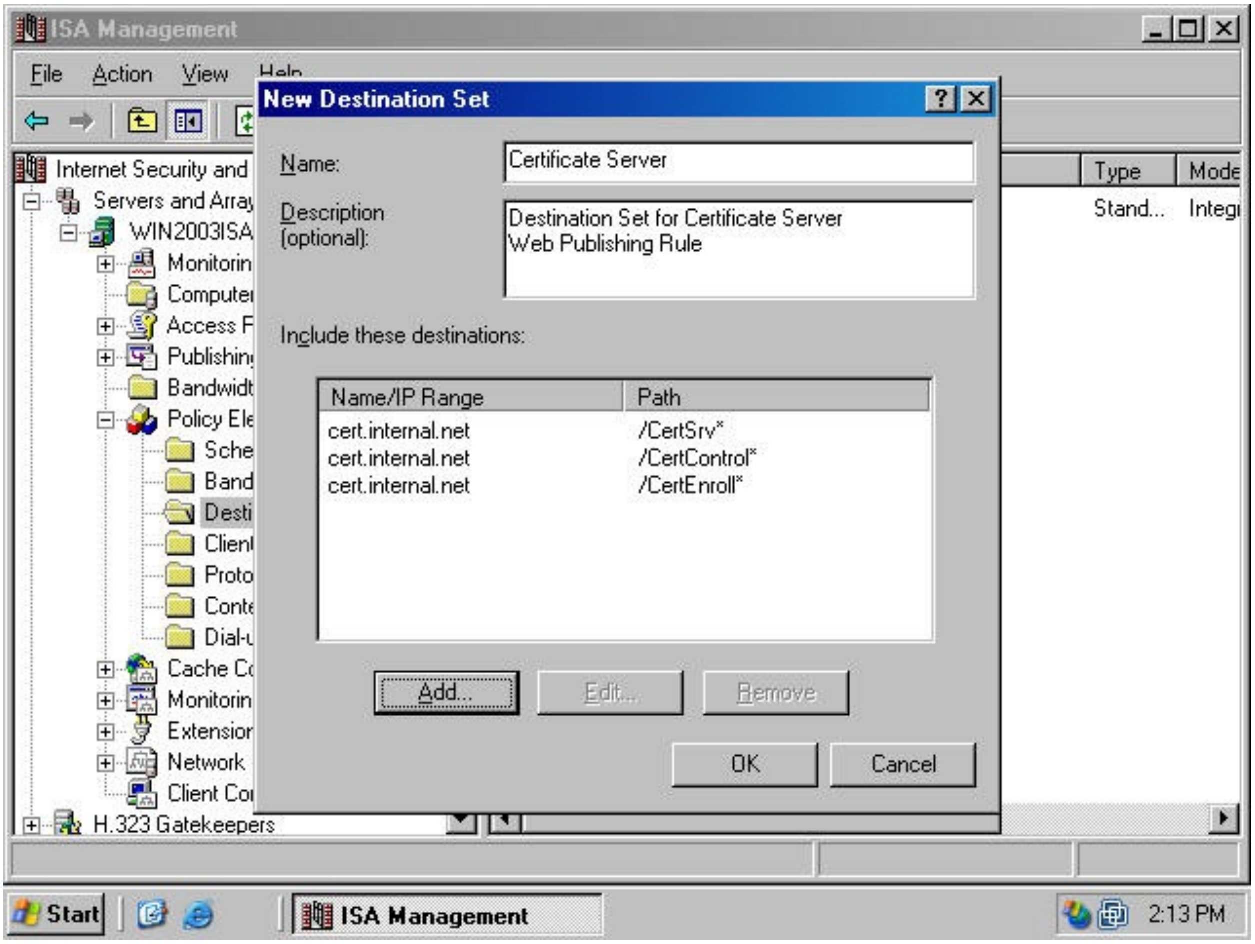
To select a specific file, use this format: /dir/filename.

Path:

/CertSrv*

8. Click **OK** in the **New Destination Set** dialog box to save the new Destination Set (figure 53).

Figure 53



New Destination Set

Name: Certificate Server

Description (optional): Destination Set for Certificate Server Web Publishing Rule

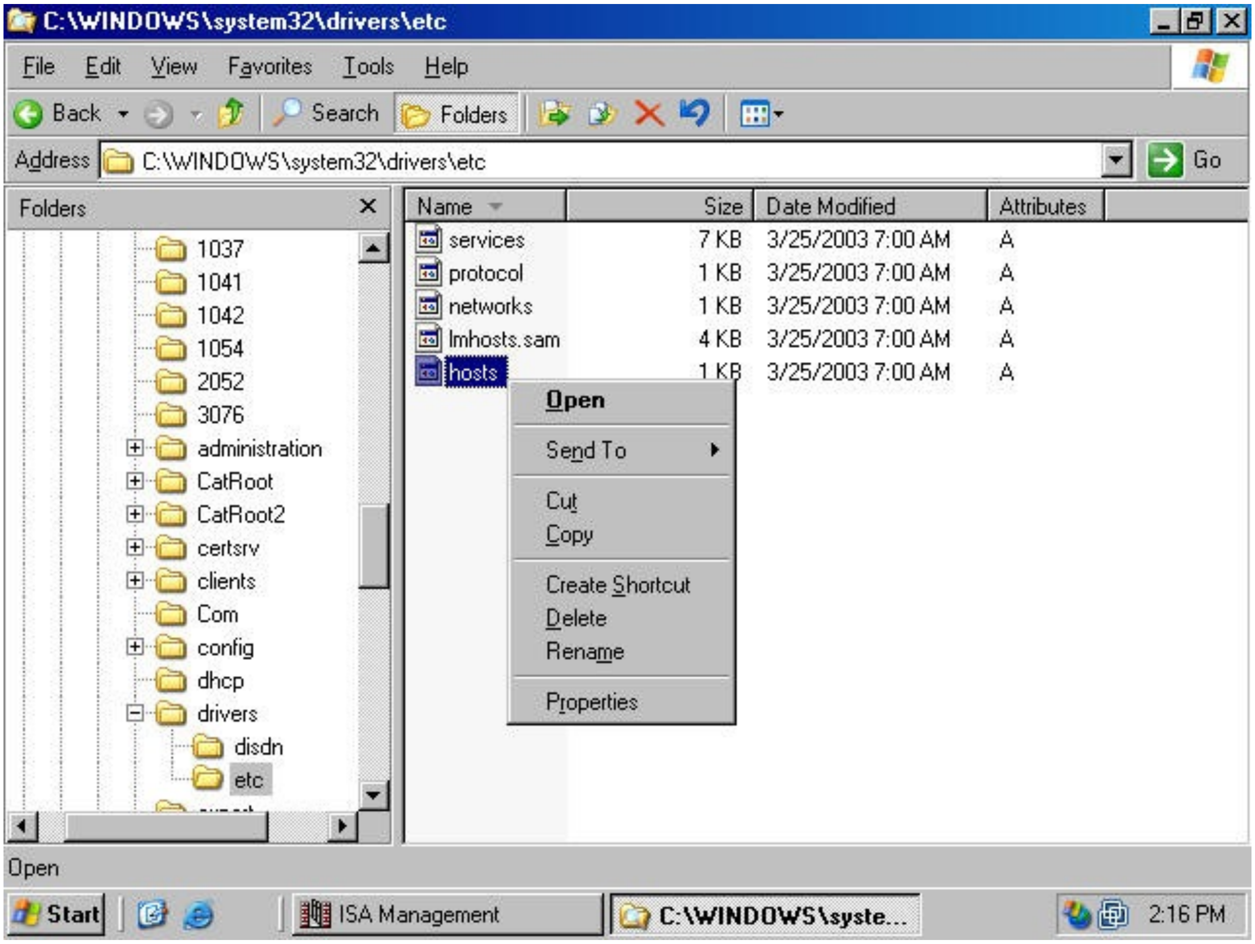
Include these destinations:

Name/IP Range	Path
cert.internal.net	/CertSrv*
cert.internal.net	/CertControl*
cert.internal.net	/CertEnroll*

The next step is to create the HOSTS file entry so that you can use the same fully qualified domain name that the external user uses to access the site in the redirect:

1. Open the **Windows Explorer** and navigate to the **SystemRoot\system32\drivers\etc** folder (figure 54). Right click on the **Hosts** file and click on the **Open** command.

Figure 54

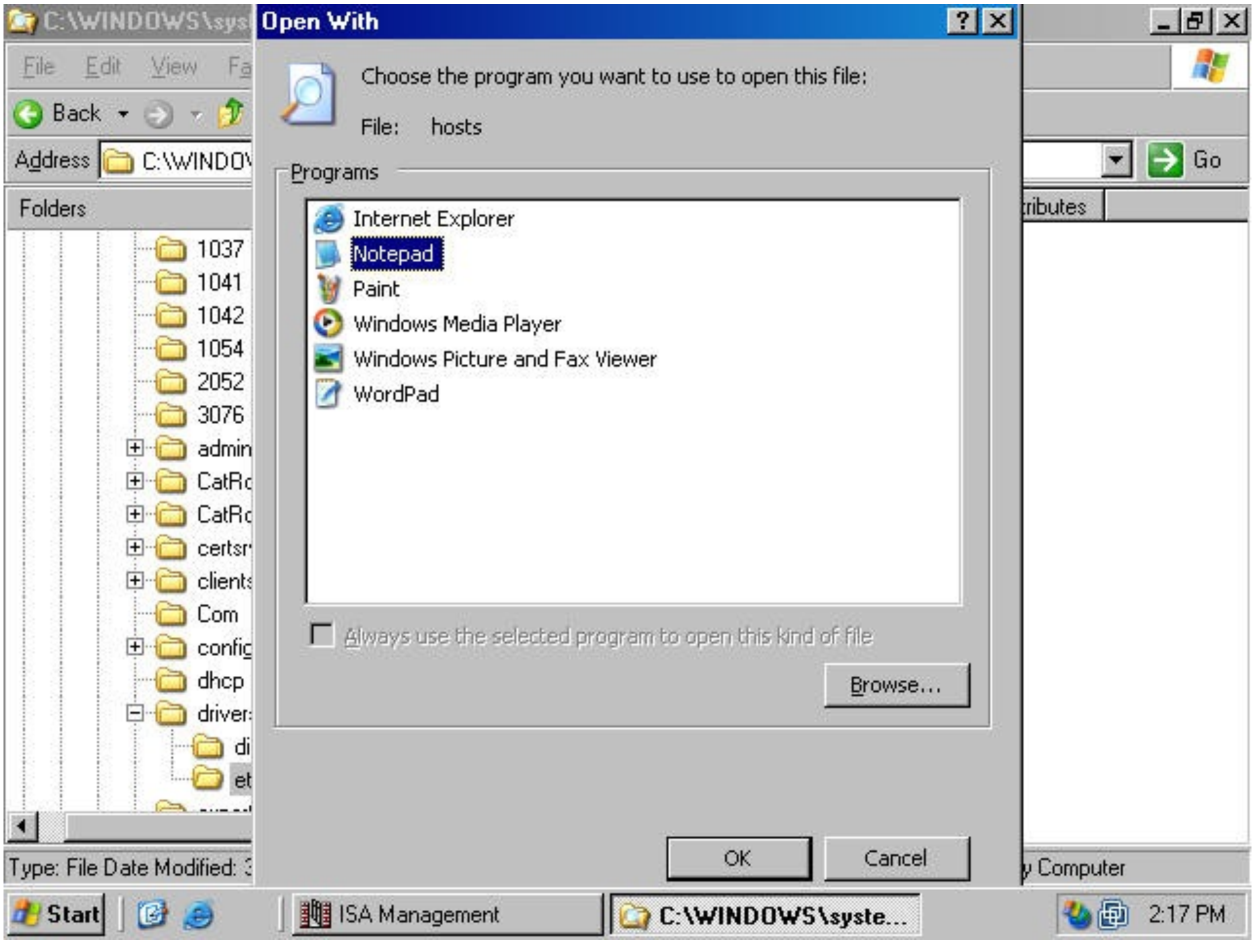


Address: C:\WINDOWS\system32\drivers\etc

Name	Size	Date Modified	Attributes
services	7 KB	3/25/2003 7:00 AM	A
protocol	1 KB	3/25/2003 7:00 AM	A
networks	1 KB	3/25/2003 7:00 AM	A
lmhosts.sam	4 KB	3/25/2003 7:00 AM	A
hosts	1 KB	3/25/2003 7:00 AM	A

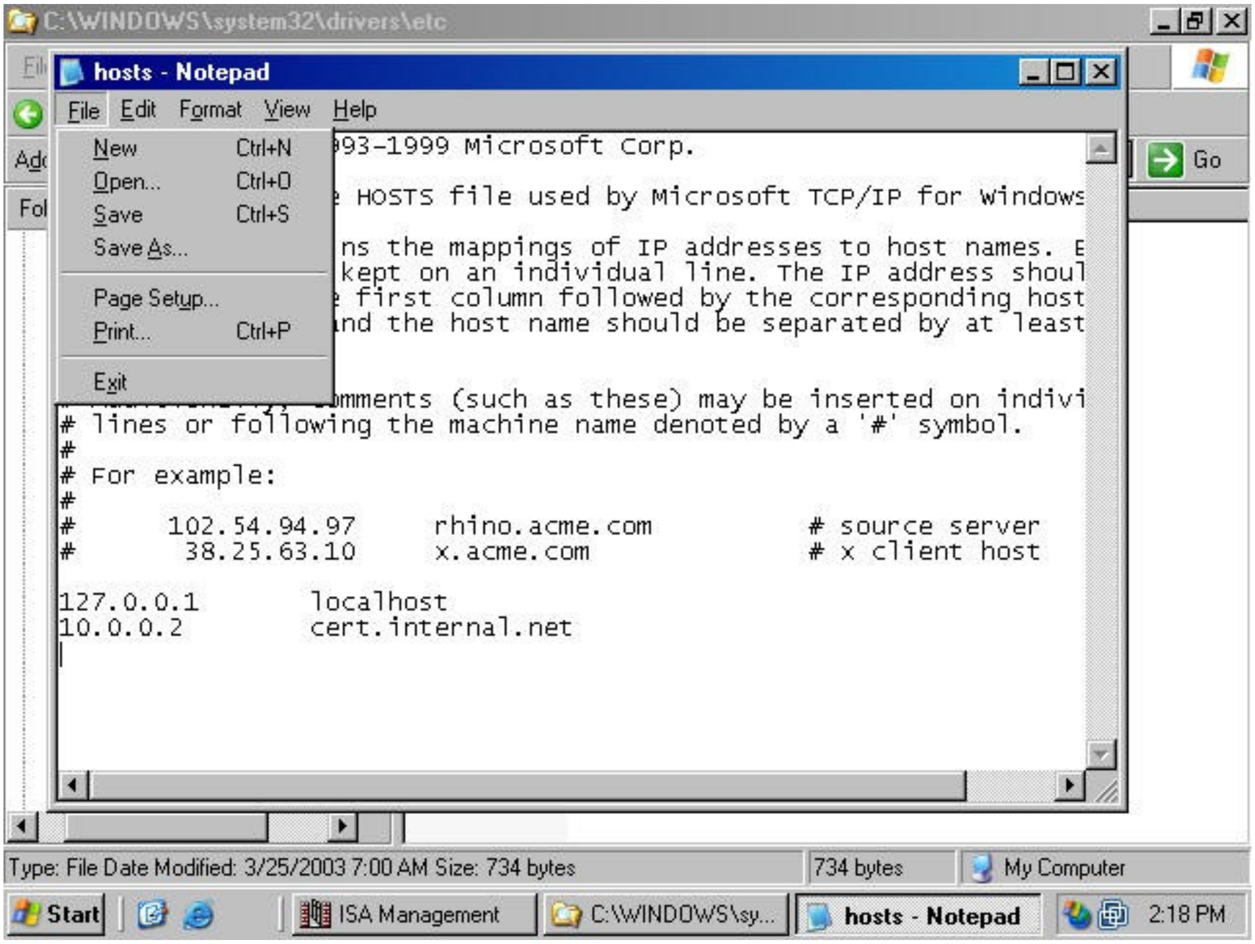
2. In the **Open With** dialog box, click on the **Notepad** entry and click **OK** (figure 55).

Figure 55



3. Type in an entry for the certificate server on the internal network. Use the same FQDN that the external users use to access the published server, but use the *internal* IP address of the server for the name mapping. In this example, the external users type http://cert.internal.net to reach the published Web enrollment site (figure 56).

Figure 56



```
                      993-1999 Microsoft Corp.

                      e HOSTS file used by Microsoft TCP/IP for Windows

                      ns the mappings of IP addresses to host names. E
                      kept on an individual line. The IP address shoul
                      e first column followed by the corresponding host
                      nd the host name should be separated by at least

                      omments (such as these) may be inserted on indivi
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
10.0.0.2        cert.internal.net
```

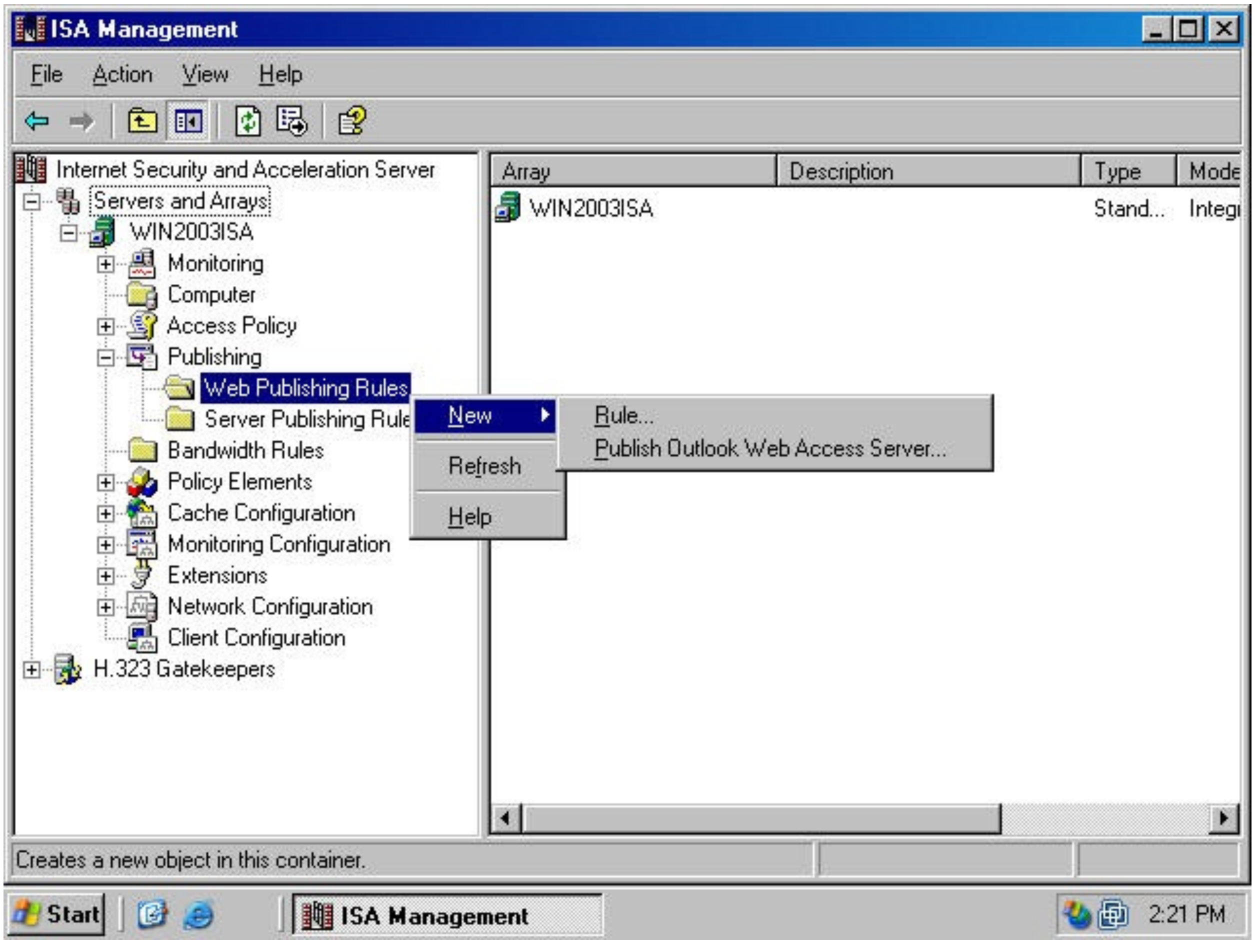
Type: File Date Modified: 3/25/2003 7:00 AM Size: 734 bytes | 734 bytes | My Computer

Create the Web Publishing Rule

All the components are now in place to create the Web Publishing Rule. Perform the following steps to create the Web Publishing Rule to publish the Certificate Server Web enrollment site:

1. In the **ISA Management** console, expand the **Servers and Array** node and then expand the server node. Expand the **Publishing** node and right click on the **Web Publishing Rules** node. Point to **New** and click on **Rule** (figure 57).

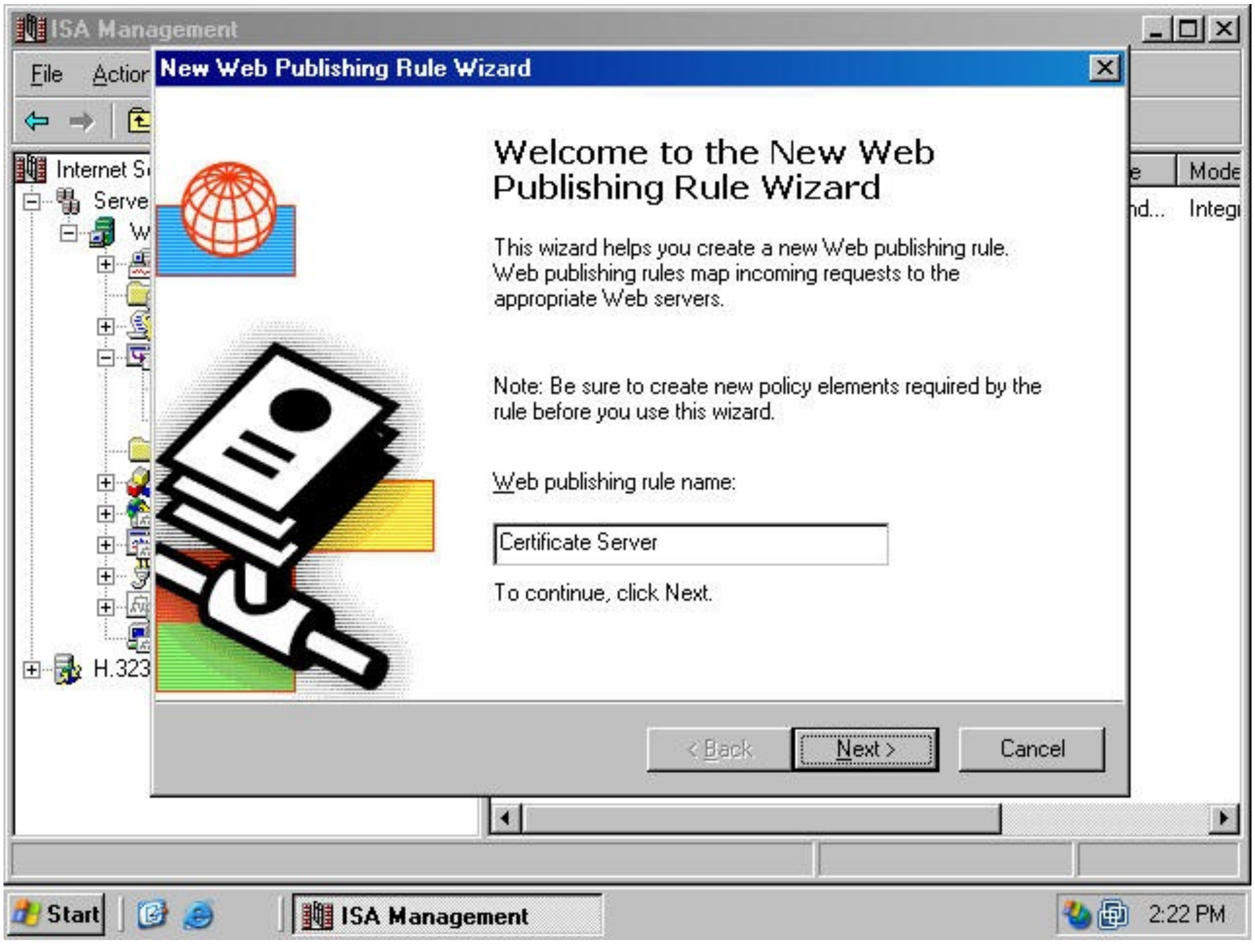
Figure 57



Creates a new object in this container.

2. Type a name for the rule in the **Web publishing rule name** text box on the **Welcome to the New Web Publishing Rule Wizard** page (figure 58). Click **Next**.

Figure 58



Welcome to the New Web Publishing Rule Wizard

This wizard helps you create a new Web publishing rule. Web publishing rules map incoming requests to the appropriate Web servers.

Note: Be sure to create new policy elements required by the rule before you use this wizard.

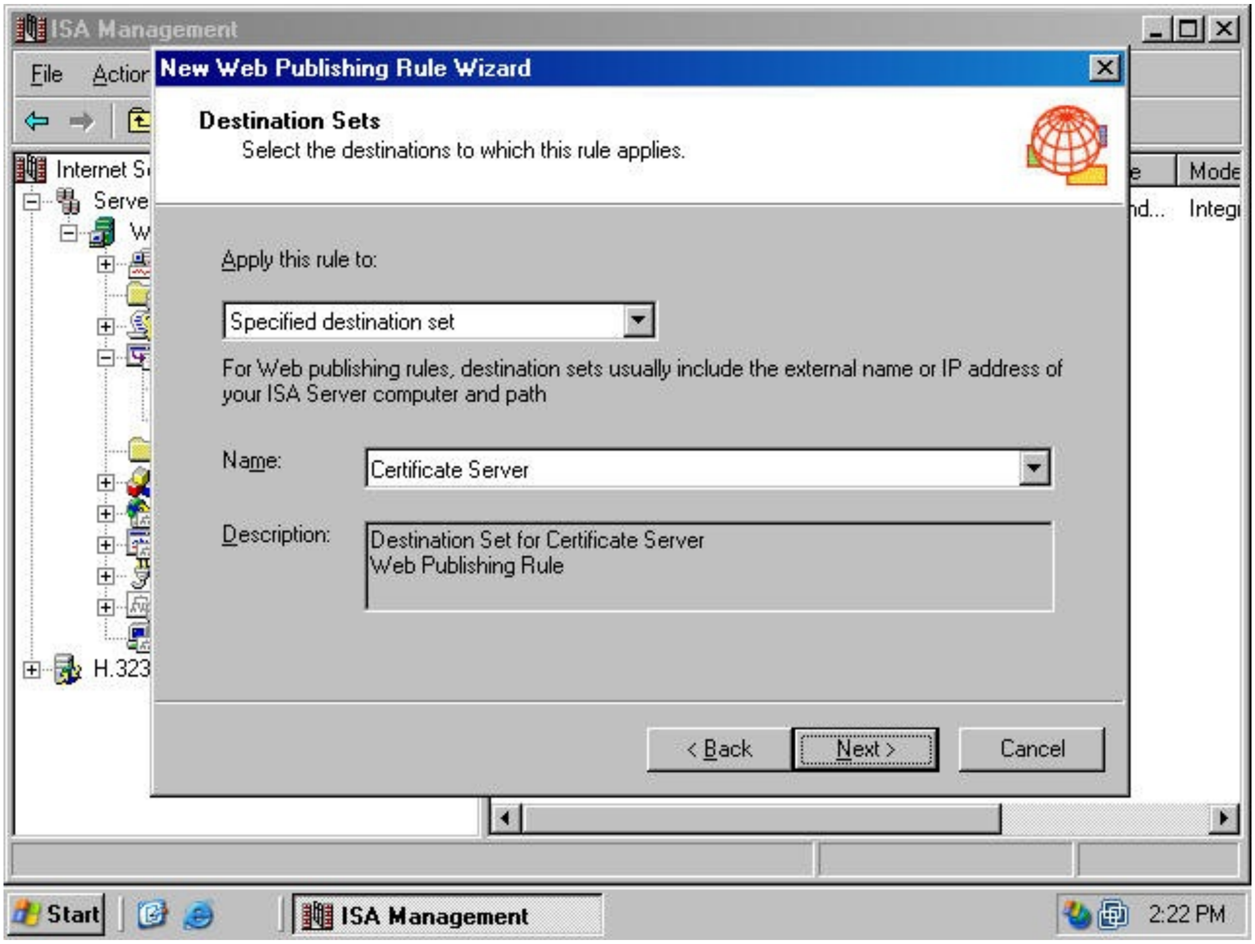
Web publishing rule name:

Certificate Server

To continue, click Next.

3. On the **Destination Sets** page, click the down arrow for the **Apply this rule to** drop down list box (figure 59) and select the **Specified destination set** option. Select the **Certificate Server** Destination Set you created earlier in the **Name** drop down list box. Click **Next**.

Figure 59



Destination Sets

Select the destinations to which this rule applies.

Apply this rule to: Specified destination set

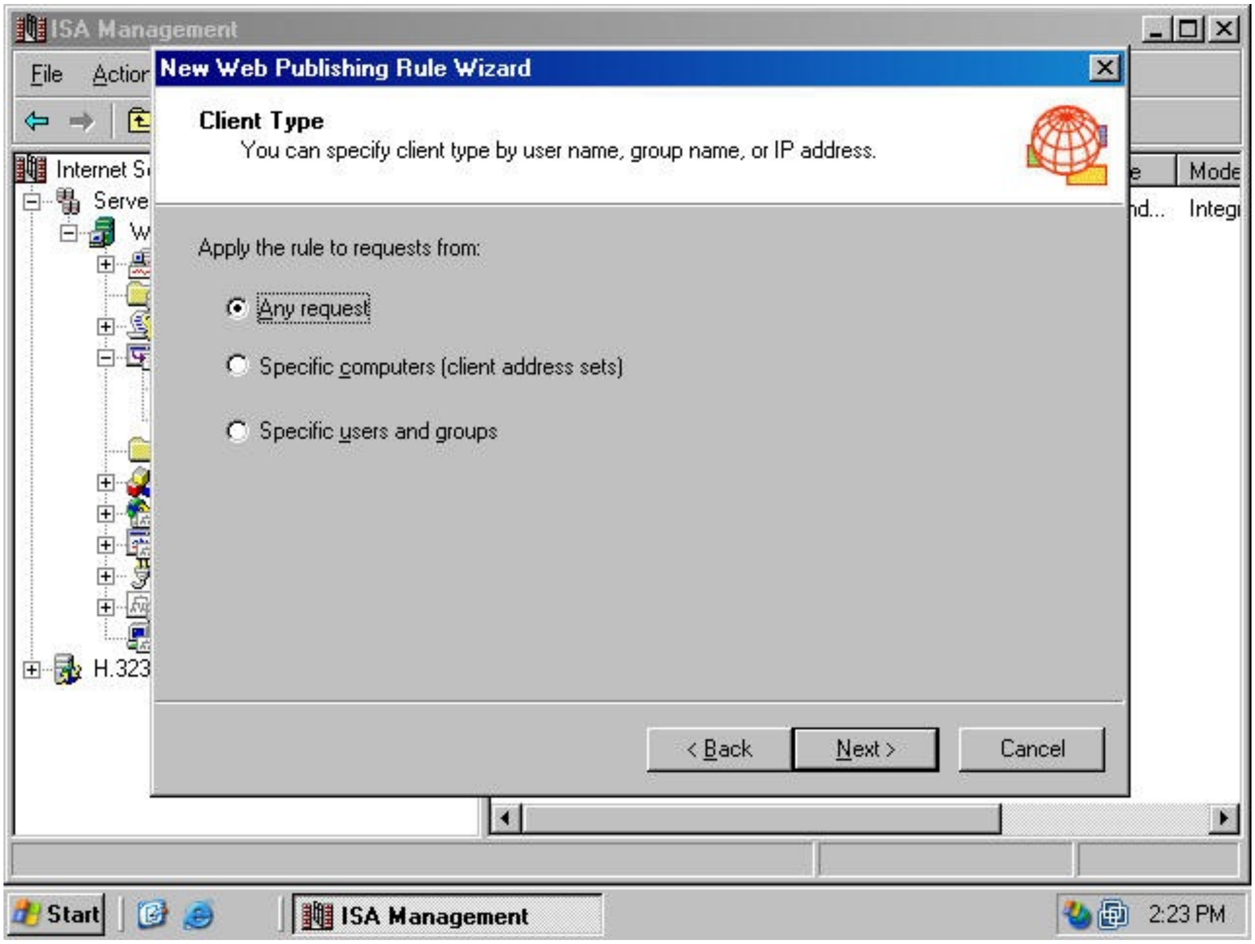
For Web publishing rules, destination sets usually include the external name or IP address of your ISA Server computer and path

Name: Certificate Server

Description: Destination Set for Certificate Server Web Publishing Rule

4. On the **Client Type** page, select the **Any request** option (figure 60). You do not want to force authentication at the Incoming Web Requests listener. Click **Next**.

Figure 60



New Web Publishing Rule Wizard

Client Type

You can specify client type by user name, group name, or IP address.

Apply the rule to requests from:

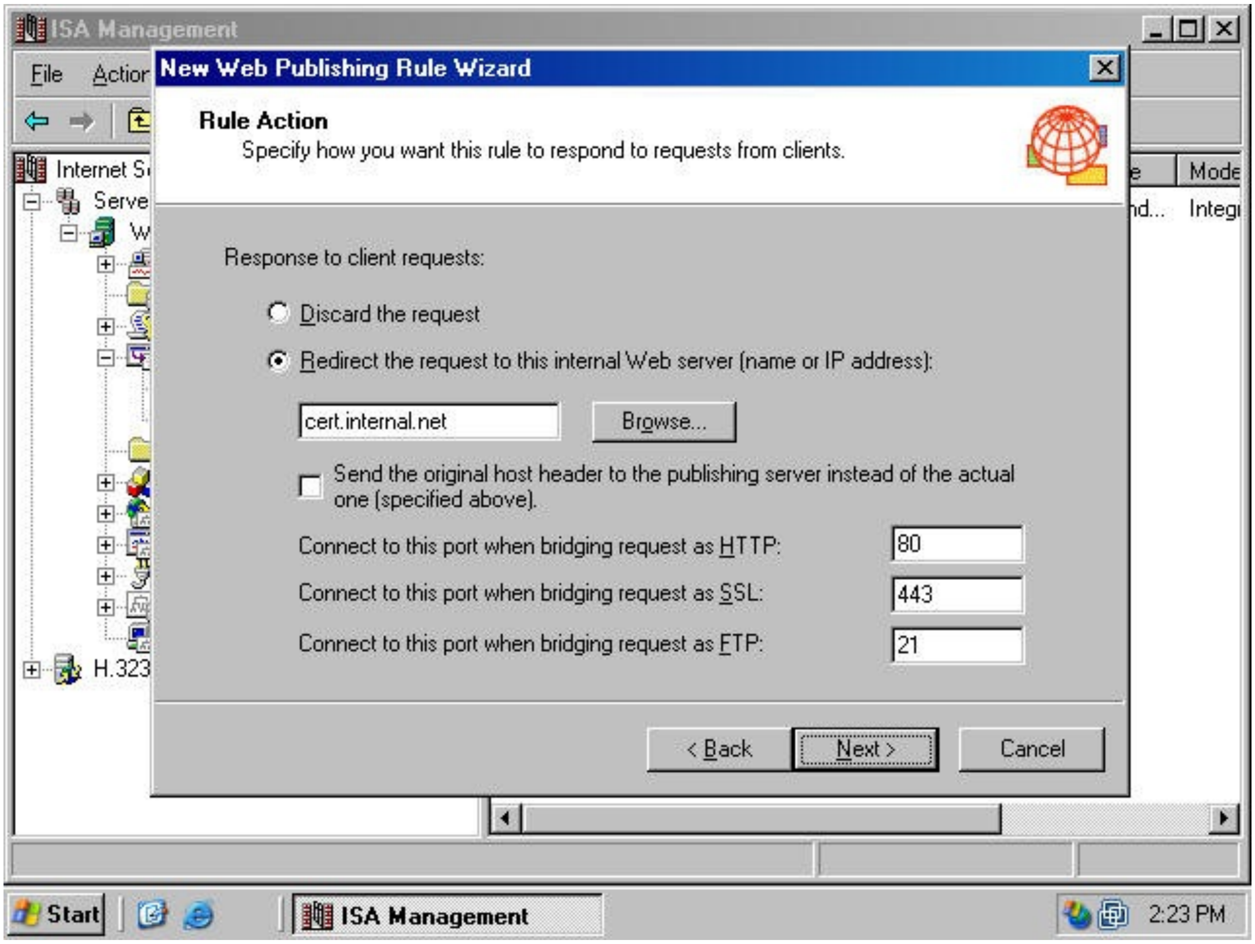
● Any request

○ Specific computers (client address sets)

○ Specific users and groups

5. On the **Rule Action** page, select the **Redirect the request to this internal Web server (name or IP address)** option (figure 61). In the text box below this option, type in the FQDN you entered in the HOSTS file. This redirects the request to the internal IP address for the published server and it will also show that the redirect to this FQDN. This will simplify your Web Proxy logs and make them more meaningful.

Figure 61



Rule Action

Specify how you want this rule to respond to requests from clients.

Response to client requests:

○ Discard the request

● Redirect the request to this internal Web server (name or IP address):

cert.internal.net

□ Send the original host header to the publishing server instead of the actual one (specified above).

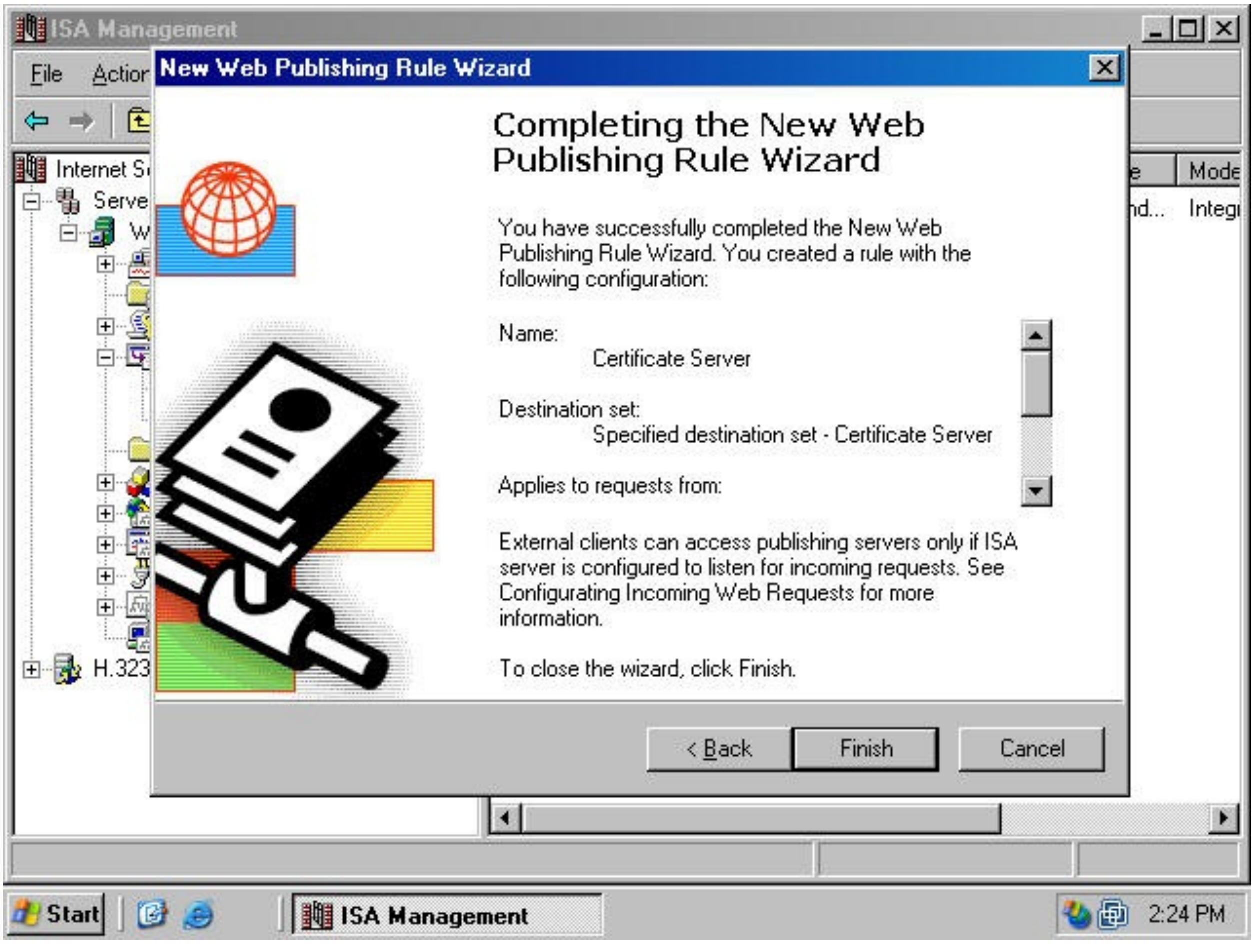
Connect to this port when bridging request as HTTP: 80

Connect to this port when bridging request as SSL: 443

Connect to this port when bridging request as FTP: 21

6. Review your settings on the **Completing the New Web Publishing Rule Wizard** page, then click the **Finish** button (figure 62).

Figure 62



Completing the New Web Publishing Rule Wizard

You have successfully completed the New Web Publishing Rule Wizard. You created a rule with the following configuration:

Name:
Certificate Server

Destination set:
Specified destination set - Certificate Server

Applies to requests from:

External clients can access publishing servers only if ISA server is configured to listen for incoming requests. See Configurating Incoming Web Requests for more information.

To close the wizard, click Finish.

The Web Publishing is effective without requiring your to restart the server or any of the ISA Server services.