Exchange 2003 RPC over HTTP Configuration on a Single Server

Information researched on Microsoft website and compiled by Matt Kuhnline
Additional screenshots and instructions by Matt Kuhnline

Prerequisites:

Server -
Exchange 2003 Service Pack 1
Windows 2003 Server
Microsoft Certificate Services 2003 to create SSL Certificate (see pages 11 and 15 - 24)

Firewall –
Open ports 80, 443

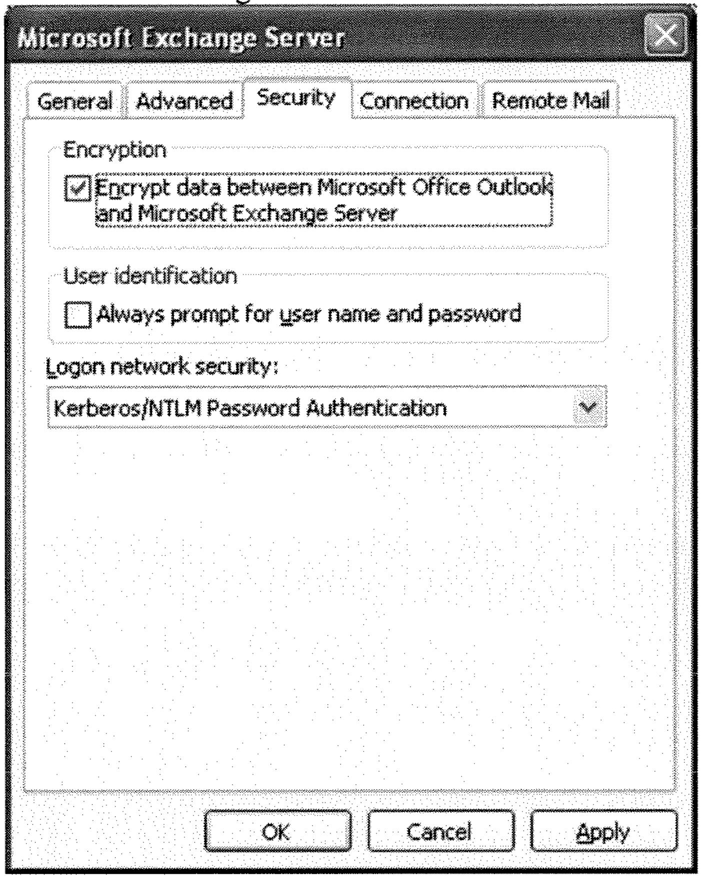
Client -
Windows XP Pro Service Pack 1 with Hotfix Q331320 *or* Service Pack 2
Outlook 2003
Add HTTP Proxy server as Trusted Certificate Authority (see page 1D, step 12)
Hotfix Q331320 can be found on Google by searching for *Q331320 Download*

Information current as of 09-14-04.

1B

Quick Client Setup Steps:

1. Make sure Windows XP (Home or Pro) SP1 is installed
2. Search Google for *Q331320 download* and download and install it. (this is included with XP SP2 so skip this if you already have SP2)
3. You must be connected to the local network of your exchange server or connected via VPN for the following steps. Once you have completed these procedures, you will not need to VPN again for Outlook.
4. Open Outlook 2003
5. Click Tools, Email Accounts, Select View or Change and click Next
6. Click your Exchange Settings and click Change
7. Click More Settings



Encryption

☑ Encrypt data between Microsoft Office Outlook and Microsoft Exchange Server

User identification

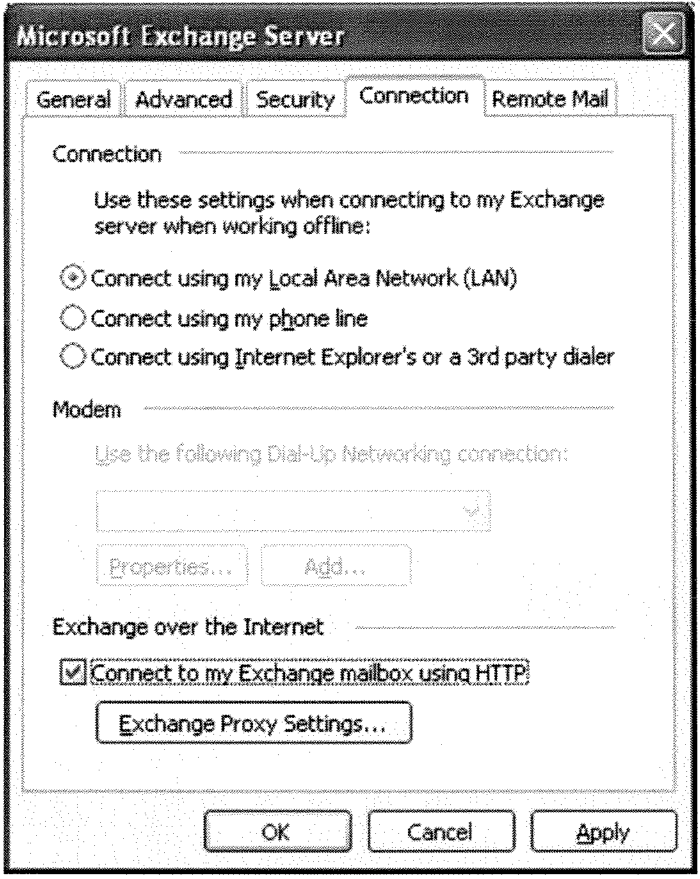
☐ Always prompt for user name and password

Logon network security: Kerberos/NTLM Password Authentication

8. Encrypt Data

1c

9. Check the box to connect via HTTP and click Exchange Proxy Settings



Connection

Use these settings when connecting to my Exchange server when working offline:

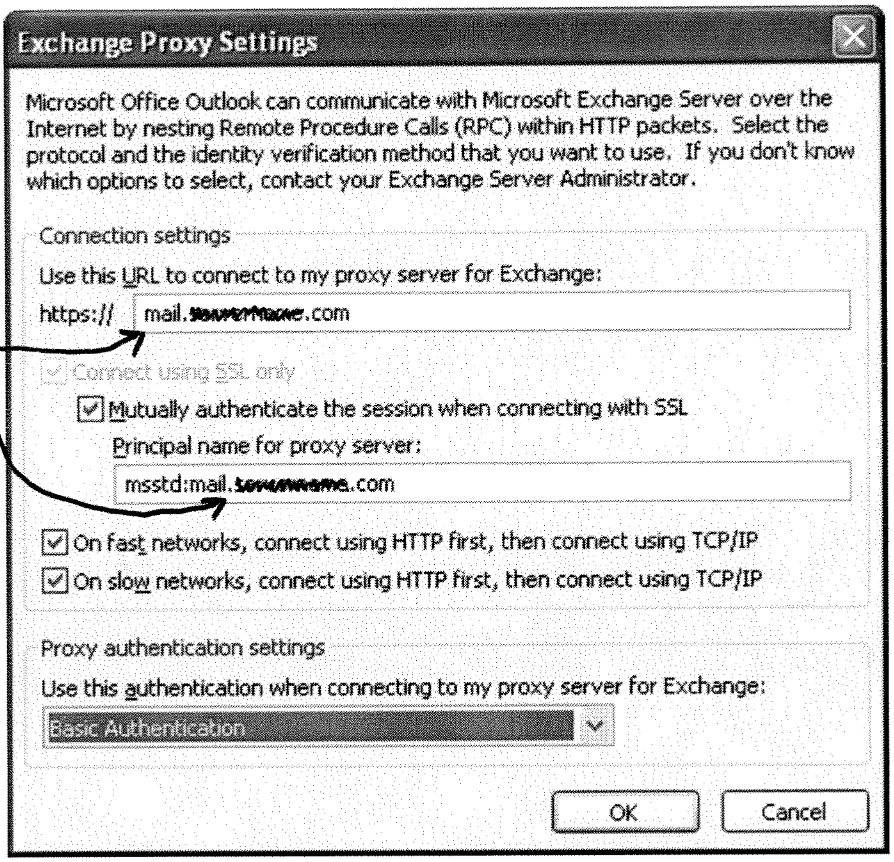
● Connect using my Local Area Network (LAN)
○ Connect using my phone line
○ Connect using Internet Explorer's or a 3rd party dialer

Modem

Use the following Dial-Up Networking connection:

Exchange over the Internet

☑ Connect to my Exchange mailbox using HTTP server FQDN



Exchange Proxy Settings

Microsoft Office Outlook can communicate with Microsoft Exchange Server over the Internet by nesting Remote Procedure Calls (RPC) within HTTP packets. Select the protocol and the identity verification method that you want to use. If you don't know which options to select, contact your Exchange Server Administrator.

Connection settings

Use this URL to connect to my proxy server for Exchange:

https:// mail.[redacted].com

☑ Connect using SSL only

☑ Mutually authenticate the session when connecting with SSL

Principal name for proxy server:

msstd:mail.[redacted].com

☑ On fast networks, connect using HTTP first, then connect using TCP/IP

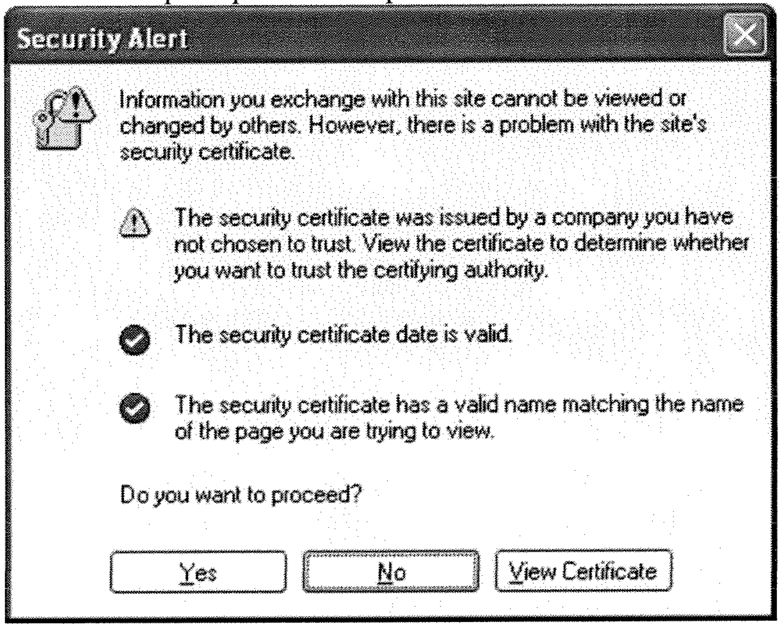
☑ On slow networks, connect using HTTP first, then connect using TCP/IP

Proxy authentication settings

Use this authentication when connecting to my proxy server for Exchange:

Basic Authentication

10. Do this:
11. Close Outlook 2003
12. Open Internet Explorer
13. Browse to your secure exchange server site https://mail.domainname.com
14. You will be prompted to accept a certificate



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

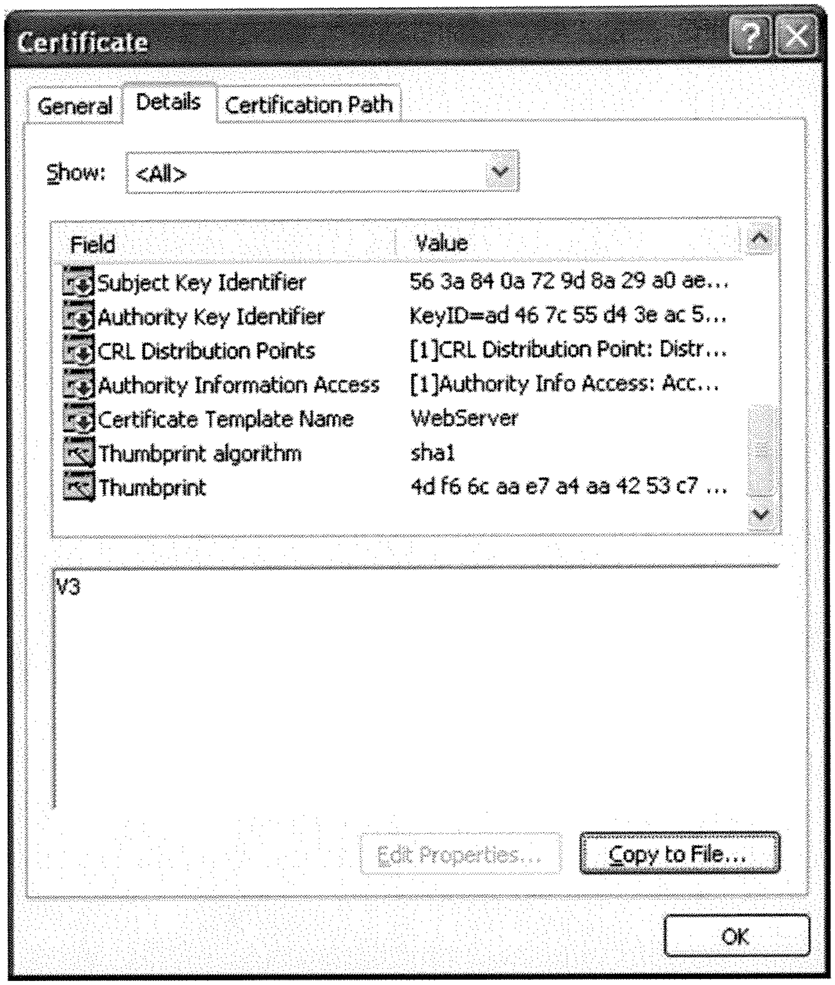
⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

✓ The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

(1E)



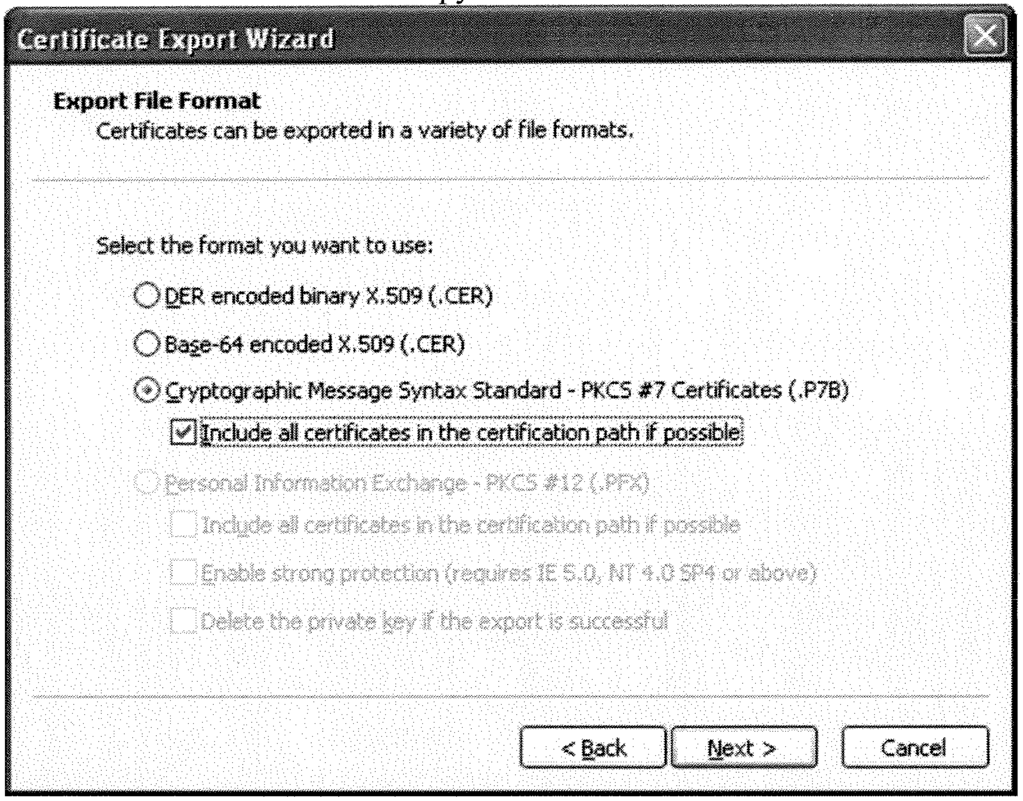
Show: <All>

Field	Value
Subject Key Identifier	56 3a 84 0a 72 9d 8a 29 a0 ae...
Authority Key Identifier	KeyID=ad 46 7c 55 d4 3e ac 5...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Certificate Template Name	WebServer
Thumbprint algorithm	sha1
Thumbprint	4d f6 6c aa e7 a4 aa 42 53 c7 ...

V3

15. Click View Certificate

16. Click the Details tab and click Copy to File



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

● Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

☑ Include all certificates in the certification path if possible

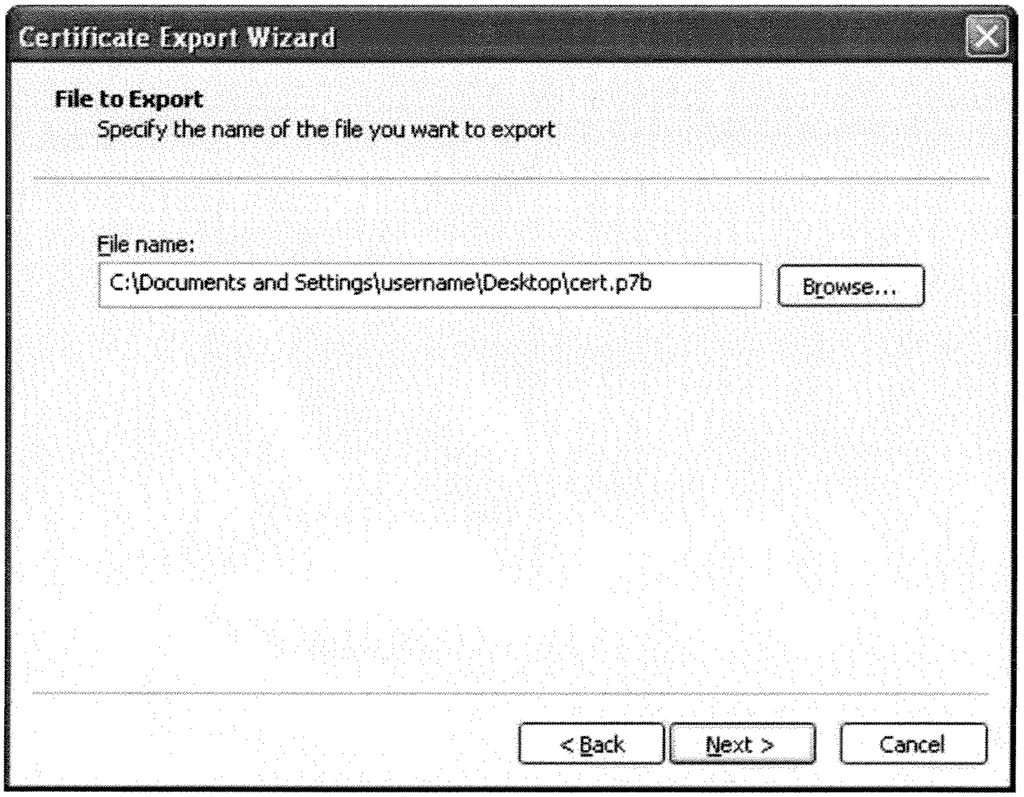
○ Personal Information Exchange - PKCS #12 (.PFX)

☐ Include all certificates in the certification path if possible

☐ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

☐ Delete the private key if the export is successful

17. Choose PKCS #7 format and click next



Certificate Export Wizard

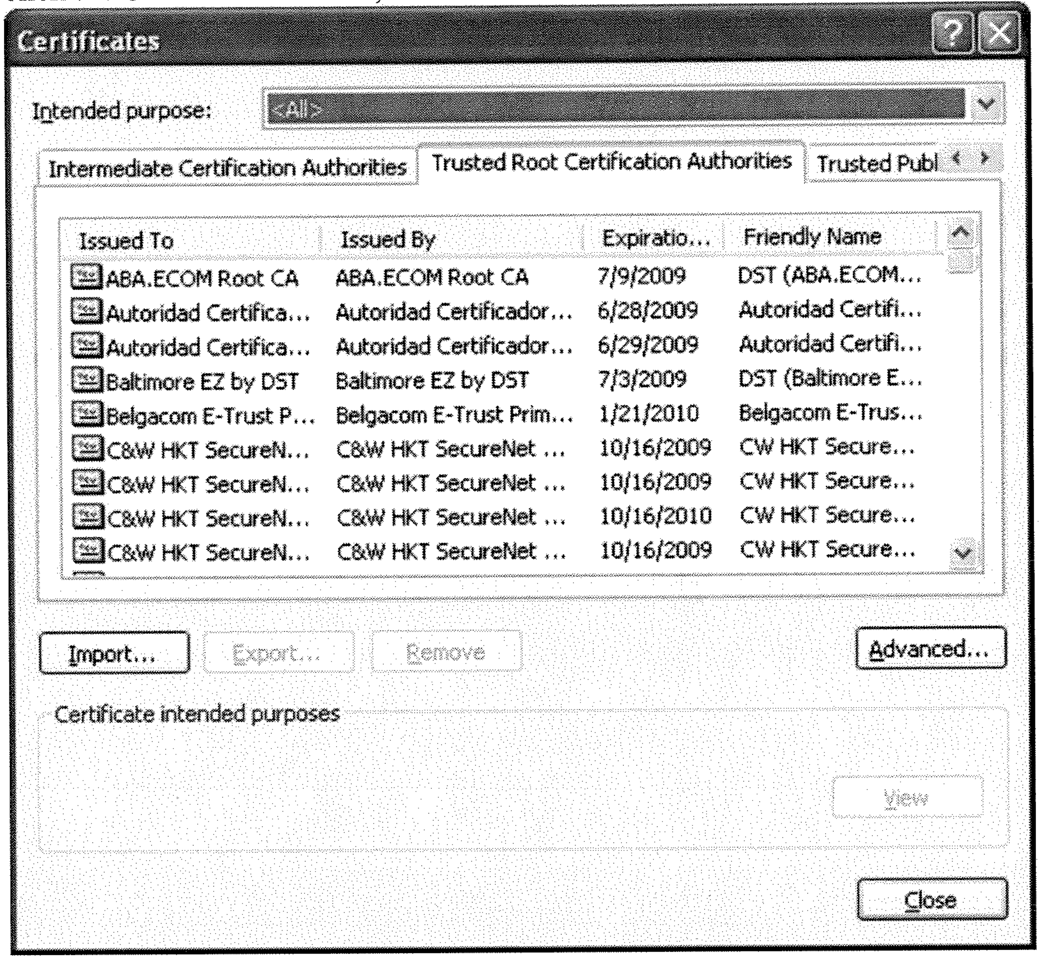
File to Export

Specify the name of the file you want to export

File name: C:\Documents and Settings\username\Desktop\cert.p7b

18. Click browse and save the certificate to your desktop so you can find it later. Once the file is saved, close internet explorer.

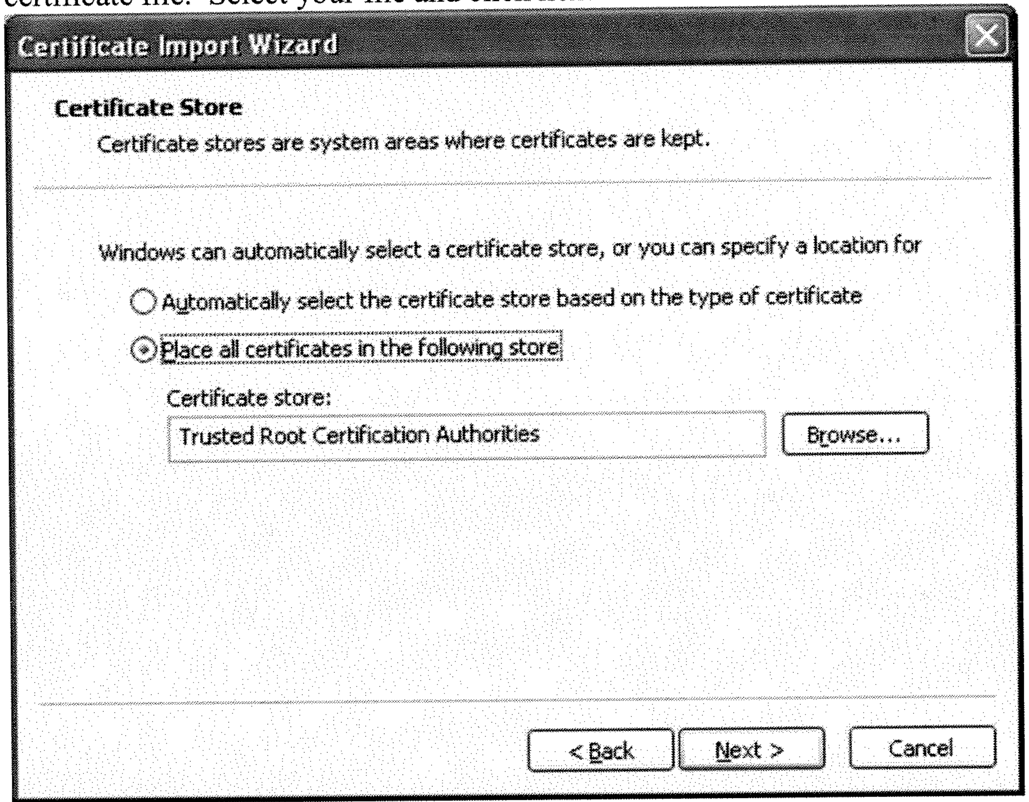
19. Open Internet Explorer again and click Tools, Internet Options, click the Content Tab and click the Certificates Button , then click the Trusted Root Certification Authorities tab.


Certificates
Intended purpose:
<All>
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Import...
Export...
Remove
Advanced...
Certificate intended purposes
View
Close

Issued To	Issued By	Expiratio...	Friendly Name
ABA.ECOM Root CA	ABA.ECOM Root CA	7/9/2009	DST (ABA.ECOM...
Autoridad Certifica...	Autoridad Certificador...	6/28/2009	Autoridad Certifi...
Autoridad Certifica...	Autoridad Certificador...	6/29/2009	Autoridad Certifi...
Baltimore EZ by DST	Baltimore EZ by DST	7/3/2009	DST (Baltimore E...
Belgacom E-Trust P...	Belgacom E-Trust Prim...	1/21/2010	Belgacom E-Trus...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/2009	CW HKT Secure...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/2009	CW HKT Secure...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/2010	CW HKT Secure...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/2009	CW HKT Secure...

20. Click Import…
21. Click browse and locate your file. You will have to click the drop-down list at the bottom of the windows labeled Files of Type and select PKCS #7 before you can see your

certificate file. Select your file and click next



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

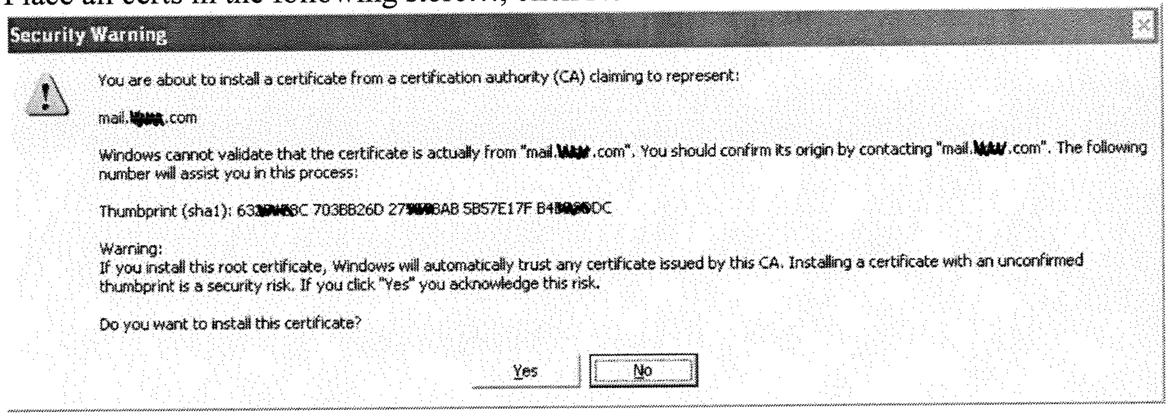
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

22. Place all certs in the following store…, click Next and Finish



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

mail.[redacted].com

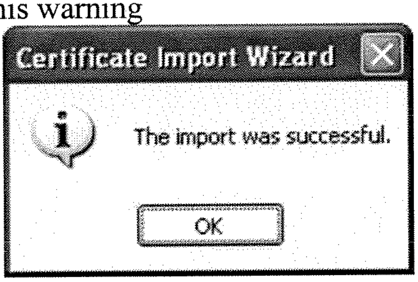
Windows cannot validate that the certificate is actually from "mail.[redacted].com". You should confirm its origin by contacting "mail.[redacted].com". The following number will assist you in this process:

Thumbprint (sha1): 63[redacted]8C 703BB26D 27[redacted]BAB 5B57E17F B4[redacted]DC

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

23. Click Yes to this warning

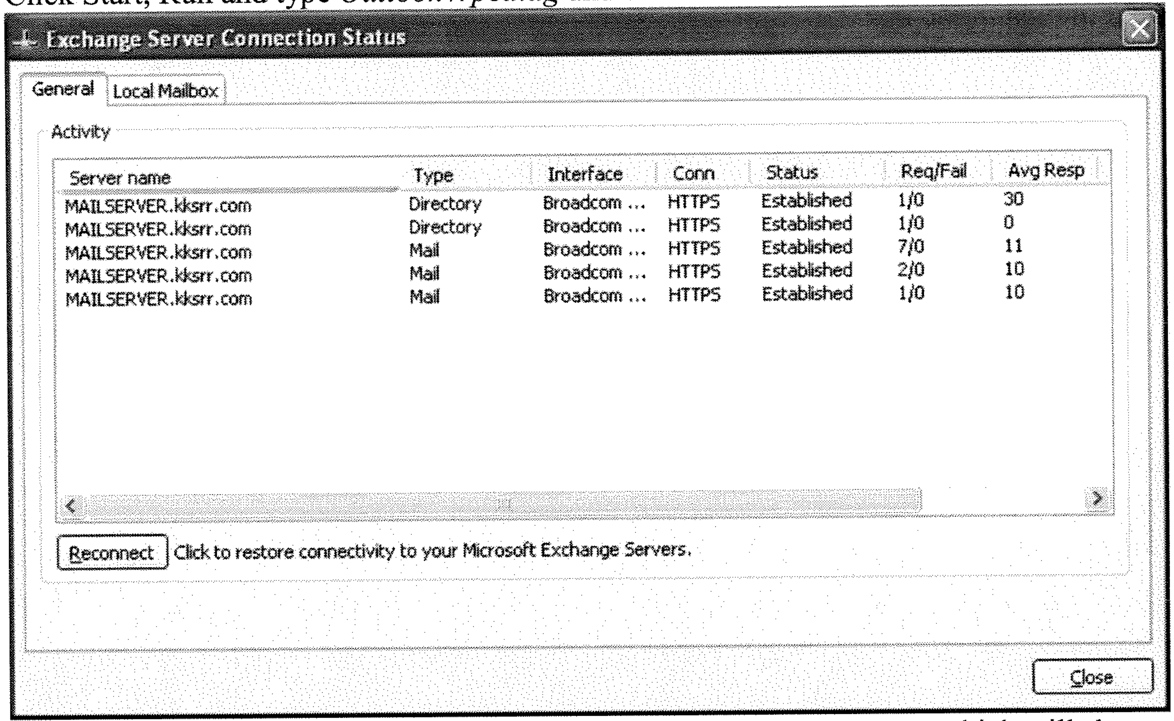


Certificate Import Wizard

The import was successful.

24. You are done.
25. Browse to your secure exchange server site again https://mail.domainname.com and it should open the page without prompting you about the certificate. Close Internet Explorer

26. Click Start, Run and type *Outlook /rpcdiag* and click OK



Server name	Type	Interface	Conn	Status	Req/Fail	Avg Resp
MAILSERVER.kksrr.com	Directory	Broadcom ...	HTTPS	Established	1/0	30
MAILSERVER.kksrr.com	Directory	Broadcom ...	HTTPS	Established	1/0	0
MAILSERVER.kksrr.com	Mail	Broadcom ...	HTTPS	Established	7/0	11
MAILSERVER.kksrr.com	Mail	Broadcom ...	HTTPS	Established	2/0	10
MAILSERVER.kksrr.com	Mail	Broadcom ...	HTTPS	Established	1/0	10

Click to restore connectivity to your Microsoft Exchange Servers.

27. This will lauch Outlook 2003 with the Connection Status window open which will show the status of the HTTPS connection. The image above shows an established connection. If you see this, you are finished.

2

New for Exchange Server 2003 Service Pack 1 (SP1)

Exchange Server 2003 Service Pack 1 (SP1) includes a new user interface in Exchange System Manager that enables you to configure your Exchange messaging system to use RPC over HTTP without manually modifying the registry settings. With this new interface, enabling RPC over HTTP for your organization involves doing the following steps:

③

Single-Server Installation to Use RPC over HTTP

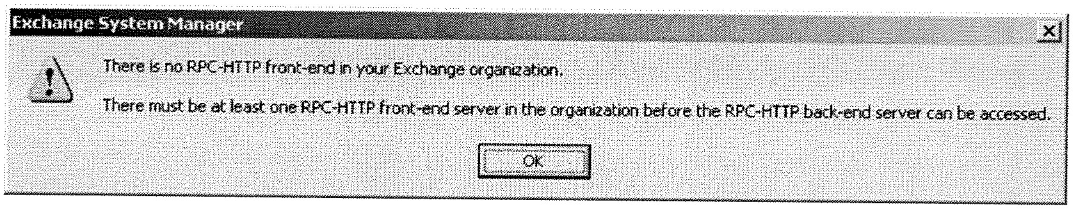
To configure an Exchange single-server installation to use RPC over HTTP, you will need to complete the following procedures:

- Configure an Exchange Server 2003 SP1 single-server installation to use RPC over HTTP
- Configure the RPC over HTTP virtual directory
- Configure the RPC proxy server to use specified ports for RPC over HTTP

> **Important** After you have completed this procedure, you will need to restart this computer for the changes to take effect.

To configure an Exchange Server 2003 SP1 single-server installation to use RPC over HTTP

1. In Exchange System Manager, expand **Administrative Groups**, and then expand the Administrative Group that contains your Exchange server.
2. Expand the **Servers** object, right-click the Exchange server you want to set as the RPC proxy server, and then select **Properties**.
3. On the **Exchange Server Properties** page, click the **RPC-HTTP** tab, and then select the option next to **RPC-HTTP back-end server**.
4. Click **OK**.
5. The following dialog box appears informing you that you do not have an Exchange front-end server in your organization. Click **OK** to close this dialog box.

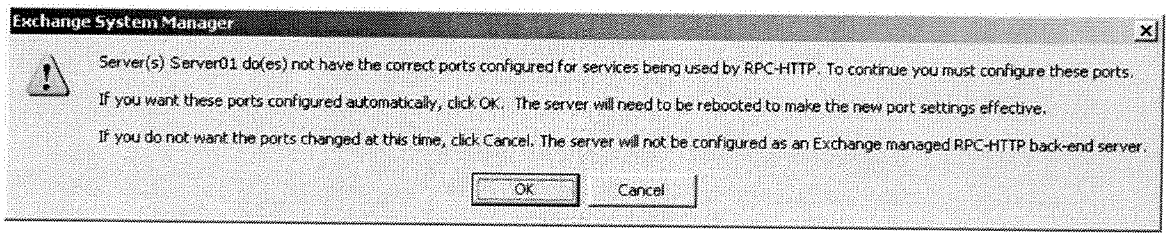


There is no RPC-HTTP front-end in your Exchange organization.

There must be at least one RPC-HTTP front-end server in the organization before the RPC-HTTP back-end server can be accessed.

Figure 10 Warning message—no front-end server configured

After you click **OK** on this dialog box, you will receive another message indicating that you can allow Exchange to configure your ports automatically to use RPC over HTTP. Click **OK** to allow Exchange to do this automatically.



Server(s) Server01 do(es) not have the correct ports configured for services being used by RPC-HTTP. To continue you must configure these ports.

If you want these ports configured automatically, click OK. The server will need to be rebooted to make the new port settings effective.

If you do not want the ports changed at this time, click Cancel. The server will not be configured as an Exchange managed RPC-HTTP back-end server.

Figure 11 Warning message—incorrect port configured

6. Restart this computer.

To configure the RPC over HTTP virtual directory

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In **Internet Information Services (IIS) Manager**, in the console tree, expand the server you want, expand **Web Sites**, expand **Default Web Site**, right-click the **RPC** virtual directory, and then click **Properties**.
3. In **RPC Virtual Directory Properties page**, on the **Directory Security** tab, in the **Authentication and access control** pane, click **Edit**.
4. On the **Authentication Methods** window, verify that the check box next to **Enable anonymous access** is cleared.

   > **Note** RPC over HTTP does not allow anonymous access by default despite what the user interface shows.
5. On the Authentication Methods window, under **Authenticated access**, select the check box next to **Basic authentication (password is sent in clear text)**, and ensure the check box next to **Integrated Windows authentication** (NTLM) is checked, and then click **OK**.
6. To save your settings, click **Apply**, and then click **OK**.
7. Ensure that you have a valid SSL certificate installed on the virtual server

Your RPC virtual directory is now ready to use Basic and NTLM authentication.

To configure the RPC proxy server to use specified ports for RPC over HTTP

The following ports are required for RPC over HTTP.

Table 1 Required ports for RPC over HTTP

Server	Ports (Services)
Exchange back-end server	6001 (store) 6002 (DSReferral) 6004 (DSProxy)

1. On the Exchange proxy server, start Registry Editor (regedit).
2. In the console tree, locate the following registry key:

   HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\RpcProxy
3. In the details pane, right-click the **ValidPorts** subkey, and then click **Modify**.
4. In **Edit String**, in the **Value data** box, type the following information:

   ```
   ExchangeServer:6001-6002;ExchangeServerFQDN:6001-
   6002;ExchangeServer:6004;ExchangeServerFQDN:6004;
   ```

   - *ExchangeServer* is the NetBIOS name of your Exchange server.
   - *ExchangeServerFQDN* is the fully qualified domain name (FQDN) of your Exchange server.

Your Exchange server is now set up to act as both a back-end mailbox and an RPC over HTTP proxy server.

⑤

Deploying RPC over HTTP for Exchange Server 2003

The following section provides detailed steps about how to deploy RPC over HTTP in your Exchange Server 2003 organization for the scenarios previously listed. Complete the steps in the following order:

1. Configure your Exchange front-end server as an RPC proxy server.
2. Configure the RPC virtual directory in Internet Information Services (IIS) on the Exchange front-end server.
3. Configure the registry on the Exchange Server 2003 computer that communicates with the RPC proxy server to use ports specified by Exchange Server 2003 for RPC over HTTP communication.
4. (Optional) Set the NTDS port for global catalog servers acting as Exchange back-end servers.
5. (Optional) Configure RPC over HTTP for SSL offloading.
6. Create an Outlook profile for your users to use with RPC over HTTP.

Each of these steps is detailed in the following sections. After you have completed these steps, your users can start using RPC over HTTP to access the Exchange front-end server.

> **Note** If you are situating your RPC proxy server inside your perimeter network, you also need to open the specified ports on the internal firewall for RPC over HTTP in addition to the standard ports for Exchange front-end communication. See "Scenario 2: Positioning the RPC Proxy Server in the Perimeter Network." This step is not detailed in the following procedures.

Instructions for installing RPC over HTTP in a single-server configuration are included in the section, "Configuring an Exchange Server 2003 Single-Server Installation to Use RPC over HTTP."

Step 1: Configuring the Exchange 2003 Front-End Server to Use RPC over HTTP

The RPC proxy server processes the Outlook 2003 RPC requests that come in over the Internet. For the RPC proxy server to successfully process the RPC over HTTP requests, you must install the Windows Server 2003 RPC over HTTP Proxy networking component on your Exchange front-end server.

To configure your Exchange front-end server to use RPC over HTTP

1. On the Exchange front-end server running Windows Server 2003, click **Start**, click **Control Panel**, and then click **Add or Remove Programs**.
2. In **Add or Remove Programs**, click **Add/Remove Windows Components** in the left pane.
3. In the Windows Components Wizard, on the **Windows Components** page, select **Networking Services**, and then click **Details**.
4. In **Networking Services**, select the **RPC over HTTP Proxy** check box, and then click **OK**.
5. On the **Windows Components** page, click **Next** to install the **RPC over HTTP Proxy** Windows component.

⑥

Step 2: Configuring the RPC Virtual Directory in Internet Information Services

Now that you have configured your Exchange front-end server to use RPC over HTTP, you must configure the RPC virtual directory in IIS.

> **Important** RPC over HTTP requires SSL to be enabled on the RPC virtual directory.

To configure the RPC virtual directory

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In **Internet Information Services (IIS) Manager**, in the console tree, expand the server you want, expand **Web Sites**, expand **Default Web Site**, right-click the **RPC** virtual directory, and then click **Properties**.
3. In **RPC Properties**, on the **Directory Security** tab, in the **Authentication and access control** pane, click **Edit**.

   > **Note** RPC over HTTP does not allow anonymous access by default despite what the user interface shows.
4. On the **Authentication Methods** window, verify that the check box next to **Enable anonymous access** is cleared.
5. On the Authentication Methods window, under **Authenticated access**, select the check box next to **Basic authentication (password is sent in clear text)** and ensure the check box next to **Integrated Windows authentication** (NTLM) is checked, and then click **OK**.
6. To save your settings, click **Apply**, and then click **OK**.

Your RPC virtual directory is now ready to use Basic and NTLM authentication.

Step 3: Configuring the RPC Proxy Server to Use Specified Ports

After you enable the RPC over HTTP Windows networking component for IIS, you can configure the RPC proxy server to use a specific number of ports to communicate with the servers in the corporate network. In this scenario, the RPC proxy server will be configured to use specified ports, and the individual computers that the RPC proxy server communicates with will also be configured to use specified ports when receiving requests from the RPC proxy server. When you run Exchange Server 2003 Setup, Exchange is automatically configured to use the ports listed in Table 2.

> **Warning** Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

To configure the RPC proxy server to use specified ports for RPC over HTTP

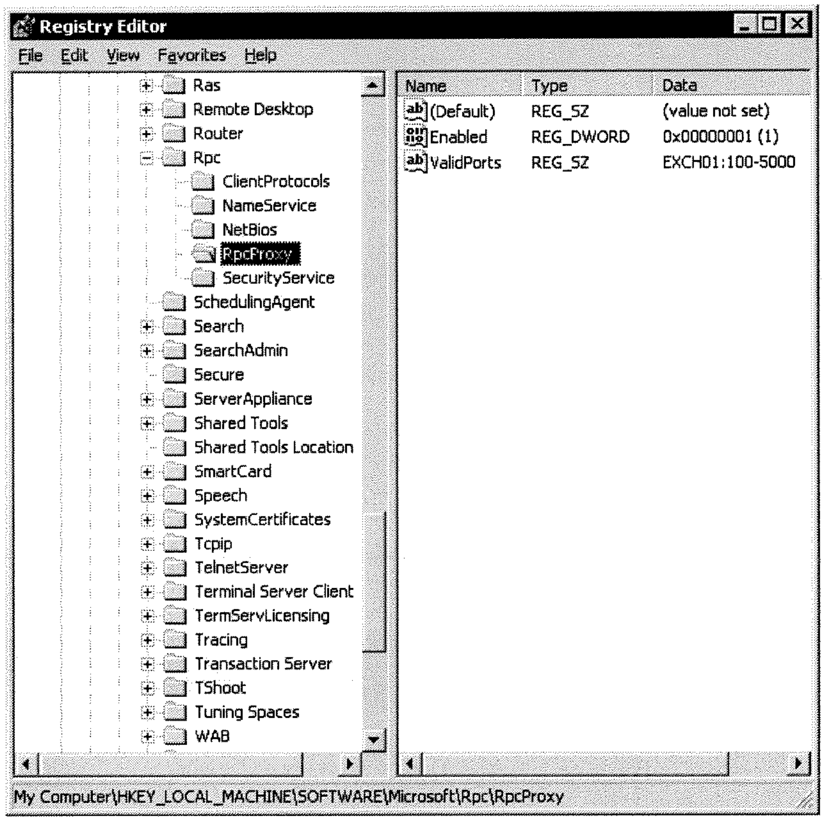
The following ports are required for RPC over HTTP.

Table 2 Required ports for RPC over HTTP

Server	Ports (Services)

Exchange back-end servers	6001 (store) 6004 (DSProxy)

1. On the RPC proxy server, start Registry Editor (regedit).
2. In the console tree, locate the following registry key:
   HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\RpcProxy
3. In the details pane, right-click the **ValidPorts** subkey, and then click **Modify** (Figure 11).



Name	Type	Data
(Default)	REG_SZ	(value not set)
Enabled	REG_DWORD	0x00000001 (1)
ValidPorts	REG_SZ	EXCH01:100-5000

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\RpcProxy

Figure 11 The RpcProxy registry settings

4. In **Edit String**, in the **Value data** box, type the following information:

```
ExchangeServer:6001;ExchangeServerFQDN:6001;ExchangeServer:6004;ExchangeServerFQDN:6
004;
```

- *ExchangeServer* is the NetBIOS name of your Exchange server.
- *ExchangeServerFQDN* is the fully qualified domain name (FQDN) of your Exchange server.

In the registry key, continue to list all servers in the corporate network with which the RPC proxy server will need to communicate.

8

Step 4: Setting the NTDS Port for Global Catalog Servers Acting as Exchange 2003 Back-End Servers

If you are using your global catalog servers as Exchange back-end mailbox servers that are contacted by clients using RPC over HTTP, you will need to modify the registry setting on these servers. This step is also required if you are using a single Exchange server installation.

> **Warning** Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

To configure the global catalog server acting as an Exchange back-end server to use a specified port for RPC over HTTP

1. On the RPC proxy server, start Registry Editor (regedit).
2. In the console tree, locate the following registry key: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters**
3. Click **Edit**, click **New**, and then select **Multi String value**.
4. Create a multi-string value with the name **NSPI interface protocol sequences**.
5. Right-click the **NSPI interface protocol sequences** multi-string value and then select **Modify**.
6. In the **Value data** field, enter **ncacn_http:6004**.
7. In Registry Editor, click **File**, and then select **Exit** to save your settings.
8. You must now restart your server for the settings to be applied.

9

Step 6: Creating an Outlook Profile to Use with RPC over HTTP

For your users to use RPC over HTTP from their client computer, they must create an Outlook profile that uses the required RPC over HTTP settings. These settings enable Secure Sockets Layer (SSL) communication with Basic authentication, which is required when using RPC over HTTP.

Although optional, it is highly recommended that you use the "Use Cached Exchange Mode" option for all profiles that will connect to Exchange using RPC over HTTP.

To create an Outlook profile to use with RPC over HTTP

1. Click **Start** and then click **Control Panel**.
2. In **Control Panel**, do one of the following tasks:
    - If you are using **Category View**, in the left pane, under **See Also,** click **Other Control Panel Options**, and then click **Mail**.
    - If you are using **Classic View**, double-click **Mail**.
3. In **Mail Setup**, under **Profiles**, click **Show Profiles**.
4. In **Mail**, click **Add**.
5. In **New Profile**, in the **Profile Name** box, type a name for this profile, and then click **OK**.
6. In the **E-mail Accounts** wizard, click **Add a new e-mail account**, and then click **Next**.
7. On the **Server Type** page, click **Microsoft Exchange Server**, and then click **Next**.
8. On the **Exchange Server Settings** page, do the following steps:
    a. In the Microsoft Exchange Server box, type the name of your back-end Exchange server where your mailbox resides.
    b. Select the check box next to **Use Cached Exchange Mode** (optional, recommended).
    c. In the **User Name** box, type the user name.
    d. Click **More Settings**.
    e. On the **Connection** tab, in the **Exchange over the Internet** pane, select the **Connect to my Exchange mailbox using HTTP** check box.
    f. Click **Exchange Proxy Settings**.
9. On the **Exchange Proxy Settings** page, under **Connections Settings**, do the following steps:
    a. Enter the fully qualified domain name (FQDN) of the RPC proxy server in the **Use this URL to connect to my proxy server for Exchange** box.
    b. Select the **Connect using SSL only** check box.
    c. Next, select the **Mutually authenticate the session when connecting with SSL** check box.
    d. Enter the FQDN of the RPC proxy server in the **Principle name for proxy server** box. Use the format: **msstd:FQDN of RPC Proxy Server**.
    e. As an optional step, you can configure Outlook 2003 to connect to your Exchange server using RPC over HTTP by default by selecting the check box next to **On fast networks, connect to Exchange using HTTP first, then connect using TCP/IP**.
10. On the **Exchange Proxy Settings** page, in the **Proxy authentication settings** window, in the **Use this authentication when connecting to my proxy server for Exchange** list, select **Basic Authentication**.
11. Click **OK**.

(10)

Appendix B: Install a Root Certification Authority Certificate in the Trusted Root Certification Authority List in Internet Explorer 5.*x*

You can deliver the root certification authority certificate to the Web site users in several ways. One way is to e-mail it and have the users install it from the e-mail. Another way is to include a download page on your Web site with a link to the certificate. A corporate-wide solution is to use the Internet Explorer Administration Kit (IEAK) to push a customer Internet Explorer browser with the root certification authority certificate already installed into the **Trusted Root Certification Authorities** list. However you make the certificate available, one thing stays the same: the way you install the certificate in the **Trusted Root Certification Authorities** list in Internet Explorer, as this appendix demonstrates.

NOTE: The certificate must be installed for Internet Explorer to trust that your site certificate is not the certificate that you just created but instead the root certification authority certificate, which was created when you installed Certificate Server.

For the purposes of this document, download the certificate by using the **Certificate Servers Web** interface, which is located at http:// *<YourServerName>*/certsrv/. After you have arrived at the Welcome page, select **Retrieve the certification authority certificate or certificate revocation list**, and then click **Next**.

You now have two choices:

- **Install this certification authority certification path**. If you are installing the root certification authority certificate into the browser that you are currently connected with, click the **Install this certification authority certification path** link, and the root certification authority certificate is automatically installed in the **Trusted Root Certification Authorities** list in your Internet Explorer browser.

  After the installation is complete, you receive a confirmation page. -or-

A

* Do This on all Client Computers

- **Download certification authority certificate**. If you must install the root certification authority certificate in the root certification authorities list in any other Internet Explorer browser, you can download it and install it as follows:
  1. Click **Download certification authority certificate**.
  2. Select **Save the file to disk**.
  3. Access the location where you saved the root certification authority certificate, and then double-click the certificate to open the Properties window for that certificate.
  4. Click **Install Certificate** to start the Certificate Import Wizard. Click **Next** to continue.
  5. Select **Place all certificates in the following store**.
  6. Click **Browse**, select **Trusted Root Certification Authorities**, and then click **Next**.
  7. Verify the settings, and then click **Finish**.

     You receive the following message:

     > The import was successful.

  8. Click **OK** to dismiss this message, and then click **OK** to close the Properties window.

  To see if you receive the trusted root certification authority warning again, close and reopen your browser, and then open the following Web site:

  https:// *<MySecureWebsite>*/Postinfo.html

  NOTE: The Postinfo.html page is a standard HTML page that is found in the root of the default Web site.

  If you can open this site, you have successfully added your root certification authority to the **Trusted Root Certification Authorities** list in your Internet Explorer browser.

B [The certificate name Must match the name of the server external FQDN (mail.domain.com)]

This name is also used in the Exchange Proxy settings in Outlook

- Obtain a certificate from a third-party certification authority (CA).

To enable and to require SSL for all communications between the RPC proxy server and the Outlook clients, you must obtain and publish a certificate at the default Web site level. We recommend that you purchase your certificate from a third-party certification authority whose certificates are trusted by a wide variety of Web browsers.

*

Important As an alternative, you can use the Certification Authority tool in Windows to install your own certification authority. By default, Web browsers do not trust your root certification authority in this scenario. When a user tries to connect in Outlook 2003 by using RPC over HTTP, that user loses the connection to Exchange. The user is not notified. The user loses the connection when one of the following conditions is true:

- A The client does not trust the certificate.
- B The certificate does not match the name that the client tries to connect to.
- The certificate date is incorrect.

See Page 10

Therefore, you must make sure that the client computers trust the certification authority. For additional information about how to trust a root certification authority, click the following article number to view the article in the Microsoft Knowledge Base:

297681 Error message: This security certificate was issued by a company that you have not chosen to trust

For additional information, visit the following Microsoft Web site:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/sag_PKPUnCertRoot.asp

Additionally, if you use your own certification authority, when you issue a certificate to your RPC proxy server, you must make sure that the **Common Name** field or the **Issued to** field on that certificate contains the same name as the URL of the RPC proxy server that is available on the Internet. For example, the **Common Name** field or the **Issued to** field must contain a name that is similar to mail.contoso.com. The **Common Name** field or the **Issued to** field cannot contain the internal fully qualified domain name of the computer. For example, those fields cannot contain a name that is similar to mycomputer.contoso.com. For additional information, visit the following Microsoft Web site:

http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/ex2k3rpc.mspx

Note While RPC over HTTP does not require SSL, you must modify the registry to enable RPC over HTTP if you do not want to use SSL. We recommend that you enable and require SSL for your RPC over HTTP communications.

back to the top

12

Pages 12 - 14 Repeat info from earlier in this document but with more detail.

Configure the Outlook 2003 computer to use RPC over HTTP

Test the RPC virtual directory configuration on the server, and then configure an e-mail profile in Outlook 2003. To do this, follow these steps:

Step 1: Test the RPC virtual directory configuration

From a client computer, visit the RPC virtual directory to make sure that it is configured correctly. To do this, follow these steps:

1. On the client computer, start Internet Explorer, type the URL of the RPC virtual directory in the **Address** list, and then click **Go**.

   For example, type **https://mail.contoso.com/rpc**, and then click **Go**.
2. If you receive the following message, click **OK**:

   > You are about to view pages over a secure connection.
   >
   > Any information you exchange with this site cannot be viewed by anyone else on the Web.

3. If you receive a message that states that the certificate was issued by a company that you have not chosen to trust, make sure that the client computer trusts the root certification authority that issued the certificate.

   Note Typically, you receive this message when you do not configure the server to use a third-party certificate. For additional information about this issue, see the "Recommendations when you use Exchange with RPC over HTTP" section.
4. When you are prompted for your credentials, type your user name in the Universal Naming Convention (UNC) format, type your password, and then click **OK**.

   For example, type your user name in the ***domain\username*** format.

You receive the following error message:

> The page cannot be displayed
>
> HTTP Error 403.2 - Forbidden: Read access is denied.
> Internet Information Services (IIS)

This error message is the expected behavior. This error message indicates that both the server and the client sides are correctly configured.

Step 2: Configure the mail profile in Outlook 2003 to use RPC over HTTP

To use RPC over HTTP from the client computer, create an Outlook mail profile that uses the RPC over HTTP settings that are required. These settings enable SSL communication together with basic authentication. We recommend that you enable the **Use Cached Exchange Mode** option for all profiles that connect to Exchange by using RPC over HTTP. However, to test RPC over HTTP, it is best to leave this option disabled. After you test your RPC over HTTP configuration, enable **Cached Exchange** mode. To create an Outlook profile to use with RPC over HTTP, follow these steps:

1. On the client computer where Outlook 2003 is installed, click **Start**, and then click **Control Panel**.
2. If Control Panel is in Category view, click **Switch to Classic View**.
3. Double-click **Mail**, and then click **Show Profiles**.
4. Click **Add**, type a descriptive name for the profile, and then click **OK**.
5. Click **Add a new e-mail account**, and then click **Next**.
6. Click **Microsoft Exchange Server**, and then click **Next**.
7. In the **Microsoft Exchange Server** box, type the fully qualified domain name of your Exchange computer.

   For example, type ***mycomputer*.contoso.com**.
8. Click to clear the **Use Cached Exchange Mode** check box.

   Important Temporarily turn off **Cached Exchange** mode to test your configuration. We recommend that you enable **Cached Exchange** mode after you test your RPC over HTTP configuration.

13

9. In the **User Name** box, type the name of the user account that you want to use, and then click **More Settings.**

   Outlook may try to resolve the user name and the host name of the Exchange computer. If you receive an error message or if a **Check Name** dialog box appears, click **Cancel.**
10. In the **Microsoft Exchange Server** dialog box, click the **Connection** tab.
11. Click **Connect using Internet Explorer's or a 3rd party dialer**, click to select the **Connect to my Exchange mailbox using HTTP** check box, and then click **Exchange Proxy Settings**.

    If the **Exchange over the Internet** area does not appear on the **Connection** tab, see the Troubleshooting section.
12. In the **Use this URL to connect to my proxy server for Exchange** box, type the URL for your Exchange computer that users can connect to on the Internet.

    For example, type ***https://mail.example.com***.
13. Click to select the **Connect using SSL only** check box.
14. If you want to enable mutual authentication, click to select the **Mutually authenticate the session when connecting with SSL** check box, and then type the public Internet URL of your Exchange computer in the **Principal name for proxy server** box.

    Type this URL in the following format:

    msstd:*public_URL_of_the_server*

    Note You do not have to enable mutual authentication.
15. To test your RPC over HTTP configuration, click to select the **On fast networks, connect to Exchange using HTTP first, then connect using TCP/IP** check box and the **On slow networks, connect to Exchange using HTTP first, then connect using TCP/IP** check box.

    Note After you test your RPC over HTTP configuration, you might want to use only one of these options. These options specify how Outlook connects to Exchange by using RPC over HTTP. Outlook determines the connection type based on the speed of the network connection. In the default configuration, the **On fast networks, connect to Exchange using HTTP first, then connect using TCP/IP** check box is not selected. The **On slow networks, connect to Exchange using HTTP first, then connect using TCP/IP** check box is selected. In this scenario, both of the following are true:
    - If Outlook detects a fast connection, it tries to connect by using TCP. If the TCP connection is unsuccessful, Outlook tries to connect by using HTTP. A fast connection is defined as a connection that is faster than 128 kilobits per second (Kbps).
    - If Outlook detects a slow connection, it tries to connect by using HTTP. If the HTTP connection is unsuccessful, Outlook tries to connect by using TCP. A slow connection is defined as a connection that is slower than 128 Kbps or equal to 128 Kbps.

    This logic permits Outlook to connect to Exchange when a network connection is available.
16. In the **Use this authentication when connecting to my proxy server for Exchange** list, click **Basic Authentication.**
17. Click **OK**, and then click **OK**.
18. Click **Next**, click **Finish**, click **Close**, and then click **OK**.

Outlook is configured to use RPC over HTTP.

* Very Helpful

Step 3: Test the Outlook connection

Verify that Outlook connects to the Exchange computer by using RPC over HTTP. To do this, follow these steps:

1. Click **Start**, click **Run**, type **outlook /rpcdiag**, and then click **OK**.
2. Type your credentials in the **User name** box and in the **Password** box, and then click **OK**.
3. If **HTTPS** appears in the **Conn** column in the **Exchange Server Connection Status** dialog box, a service is connected by using RPC over HTTP.

back to the top

Troubleshooting

- If the **Exchange over the Internet** area does not appear on the **Connection** tab of the **Microsoft Exchange**

(14)

Server dialog box, make sure that your client computer meets the requirements to configure RPC over HTTP. If you installed the service pack and the update package that are required, and the **Exchange over the Internet** area does not appear on the **Connection** tab, edit the Windows registry. To do this, follow these steps:

1. Start Registry Editor.

   Warning If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.
2. Locate and then click the following registry subkey:

   HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Outlook\RPC

3. Create the following registry entry if it does not exist:

   Value name: EnableRPCtunnelingUI
   Value type: REG_DWORD
   Value data: 1

4. Quit Registry Editor.

- When you are prompted for your credentials, you must enter them by using the *domain*\|*username* format.
- To support the use of credentials in the user principal name (UPN) format, install the hotfix that is described in the following Knowledge Base article on each Windows XP-based client computer:

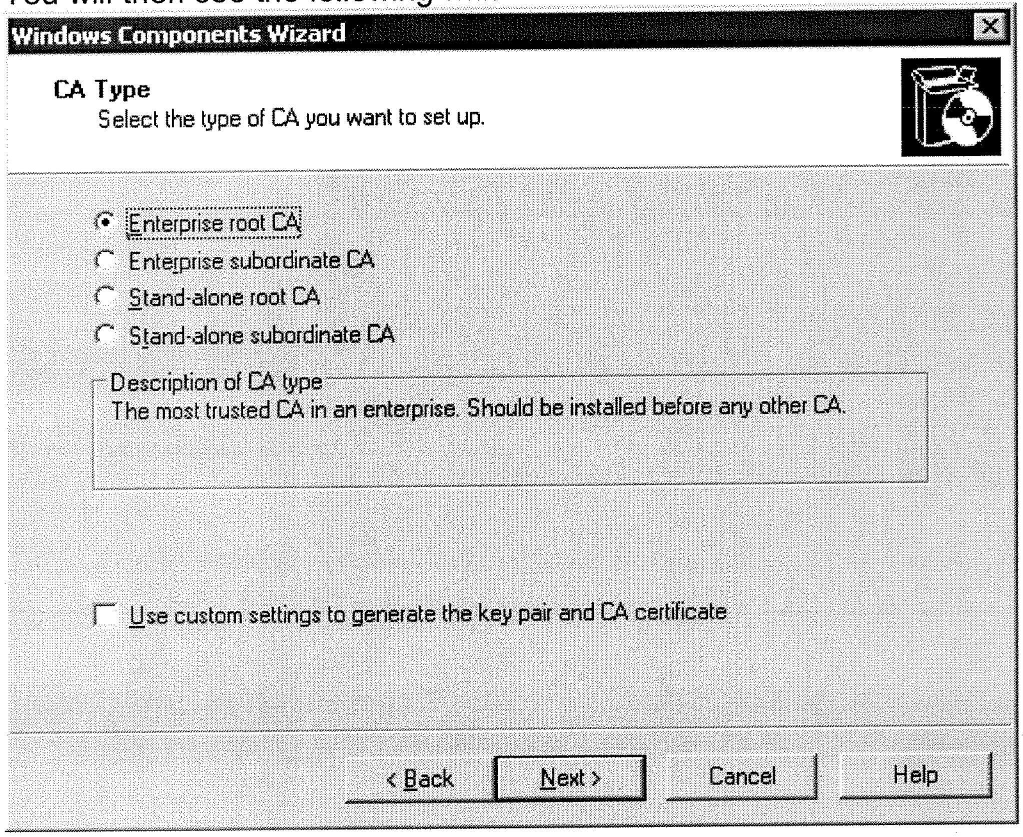
  830355 You cannot use Outlook 2003 over the Internet by using your user principal name (UPN)

The following credentials are an example of credentials in the UPN format:

username@contoso.com

How to Install Certificate Service on Windows Server 2003

On the server:
Open Control Panel, Add or Remove programs, Add/Remove Windows Components
Install "Certificate Services"
You will then see the following wizard:



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

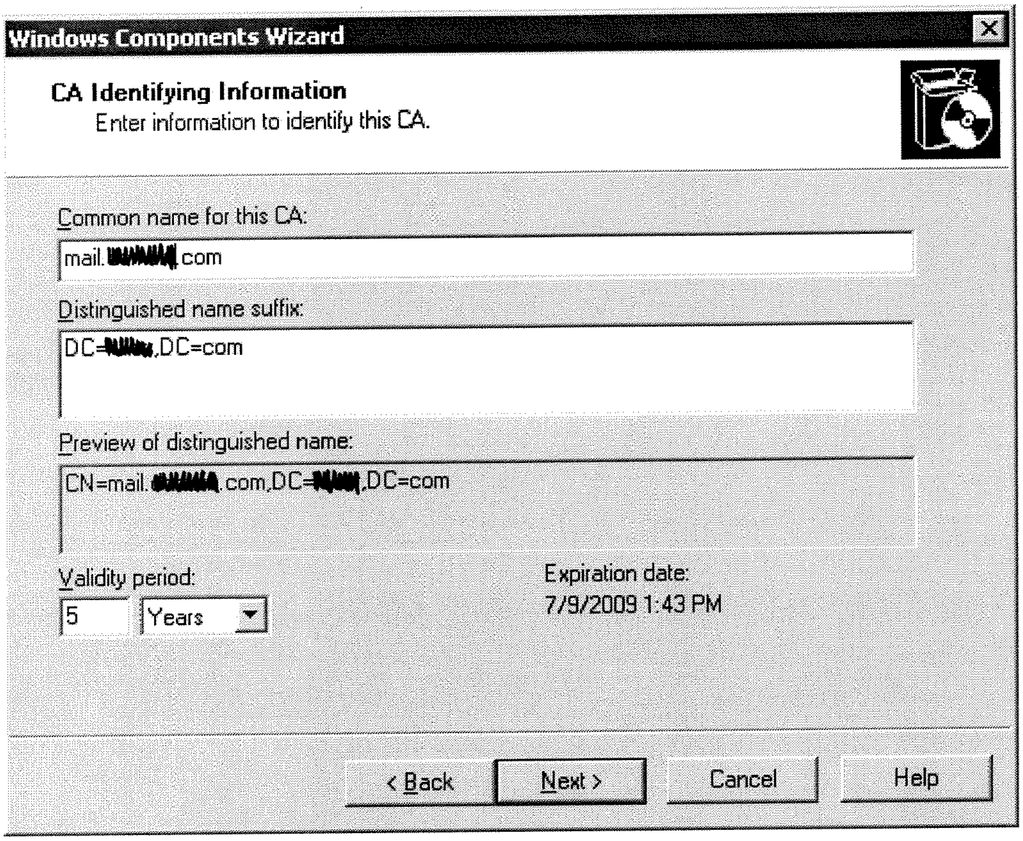
● Enterprise root CA
○ Enterprise subordinate CA
○ Stand-alone root CA
○ Stand-alone subordinate CA

Description of CA type
The most trusted CA in an enterprise. Should be installed before any other CA.

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

Note: on the following pages
the domain name has been
blacked out for security

www.[redacted].com



CA Identifying Information

Enter information to identify this CA.

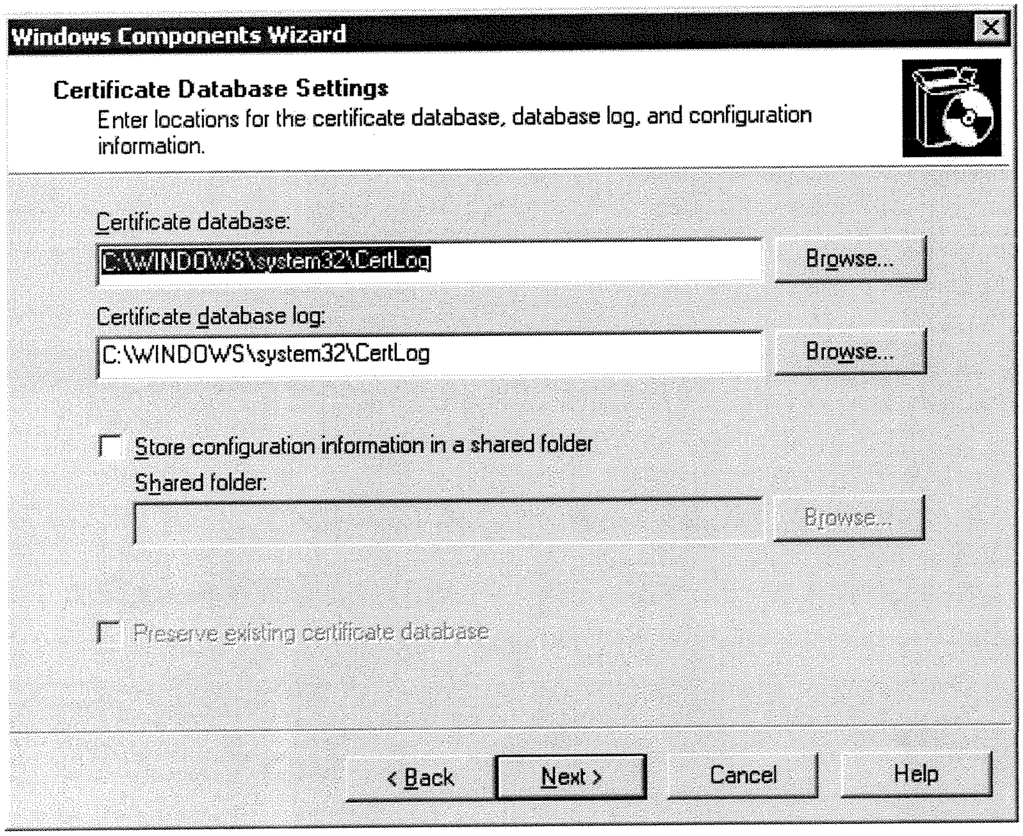
Common name for this CA: mail.[redacted].com

Distinguished name suffix: DC=[redacted],DC=com

Preview of distinguished name: CN=mail.[redacted].com,DC=[redacted],DC=com

Validity period: 5 Years

Expiration date: 7/9/2009 1:43 PM



Certificate Database Settings

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

Certificate database: C:\WINDOWS\system32\CertLog

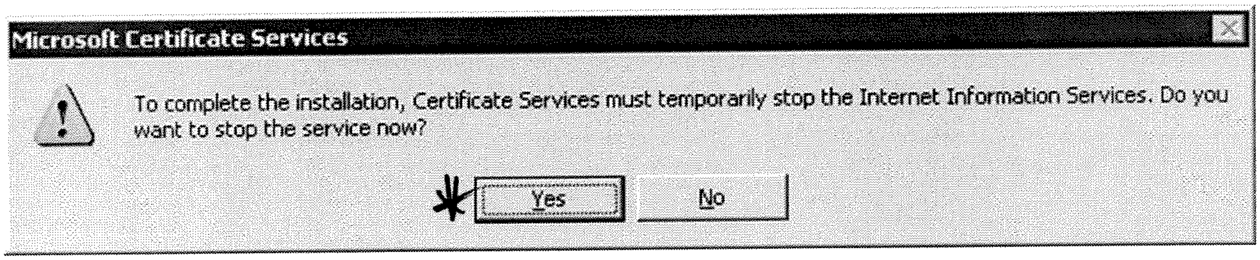
Certificate database log: C:\WINDOWS\system32\CertLog

☐ Store configuration information in a shared folder

Shared folder:

☐ Preserve existing certificate database

(17)

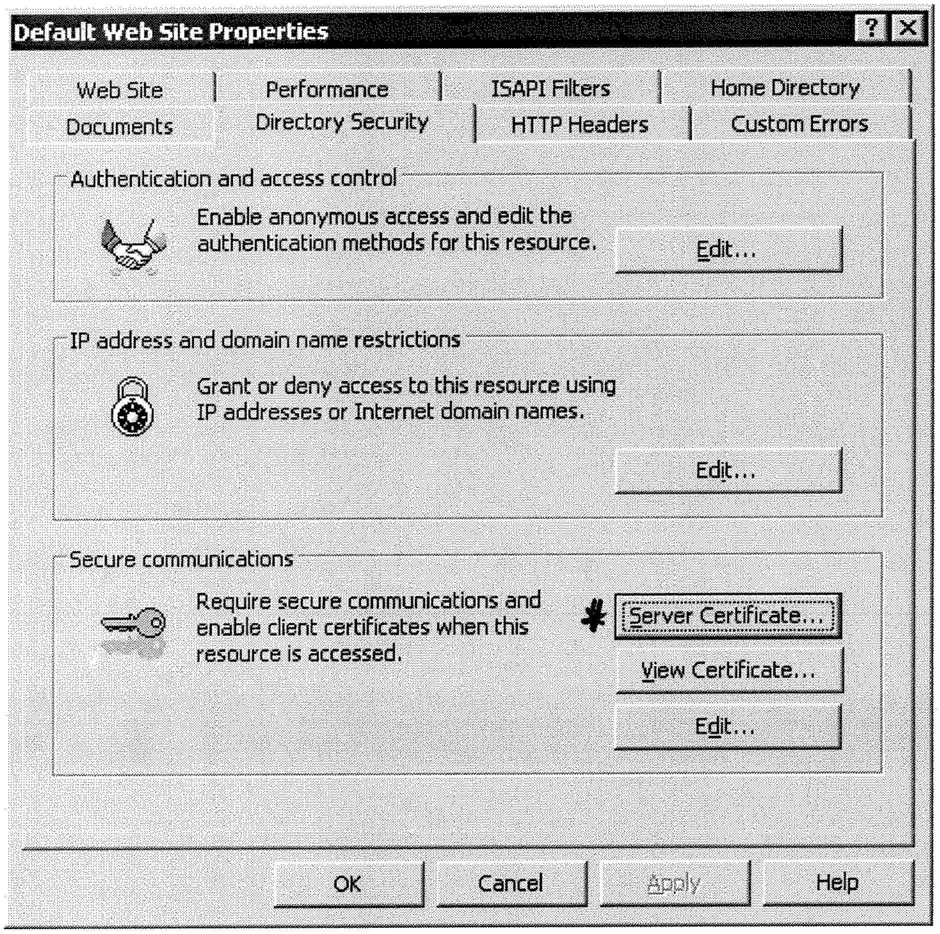


To complete the installation, Certificate Services must temporarily stop the Internet Information Services. Do you want to stop the service now?

*

Installing a Certificate on your Web Server

Open IIS Manager (under Administrative Tools)
Right-click "Default Web Site" and click Properties
Under the Directory Security Tab, click Server Certificate
Follow the wizard to create the SSL Certificate



Authentication and access control

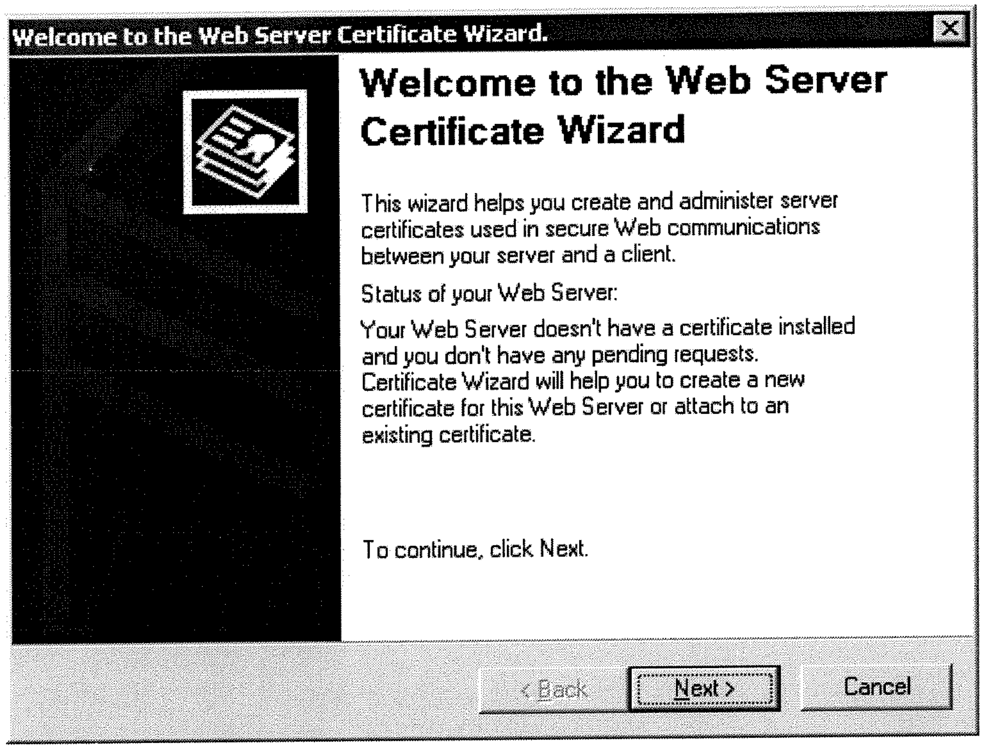
Enable anonymous access and edit the authentication methods for this resource.

IP address and domain name restrictions

Grant or deny access to this resource using IP addresses or Internet domain names.

Secure communications

Require secure communications and enable client certificates when this resource is accessed.



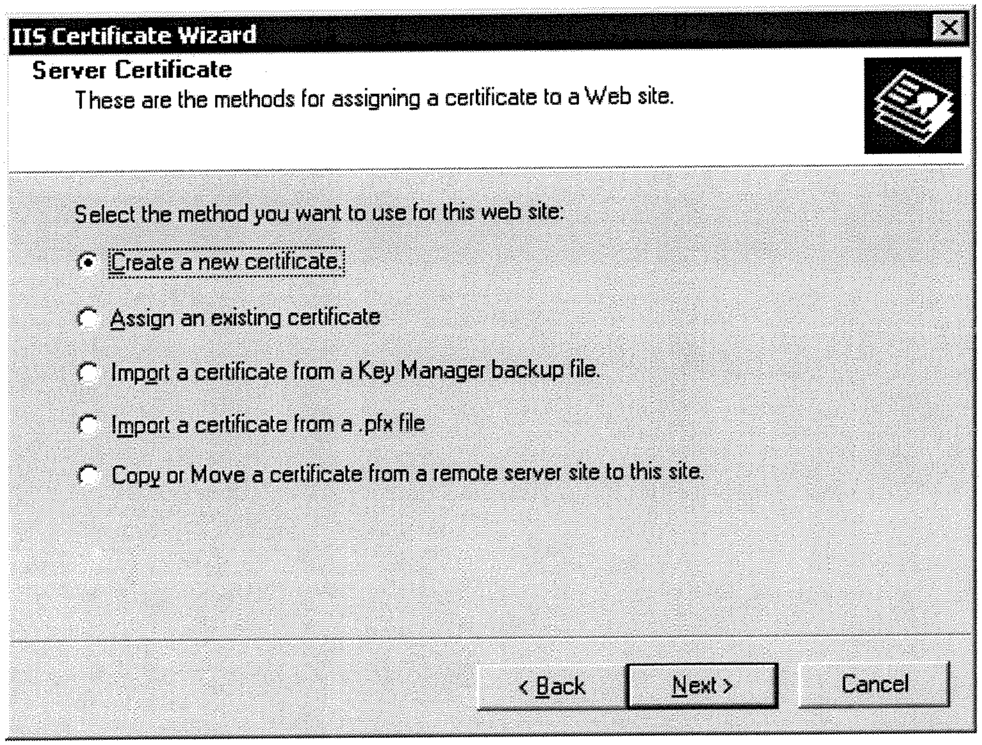
Welcome to the Web Server Certificate Wizard

This wizard helps you create and administer server certificates used in secure Web communications between your server and a client.

Status of your Web Server:

Your Web Server doesn't have a certificate installed and you don't have any pending requests. Certificate Wizard will help you to create a new certificate for this Web Server or attach to an existing certificate.

To continue, click Next.

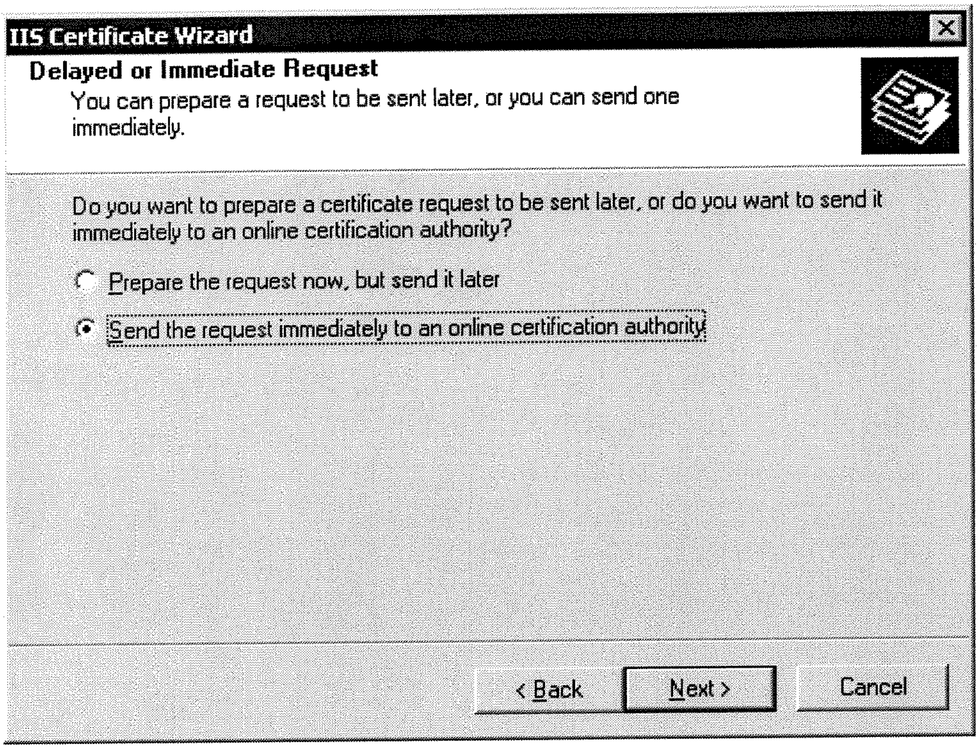


Server Certificate

These are the methods for assigning a certificate to a Web site.

Select the method you want to use for this web site:

- ● Create a new certificate.
- ○ Assign an existing certificate
- ○ Import a certificate from a Key Manager backup file.
- ○ Import a certificate from a .pfx file
- ○ Copy or Move a certificate from a remote server site to this site.



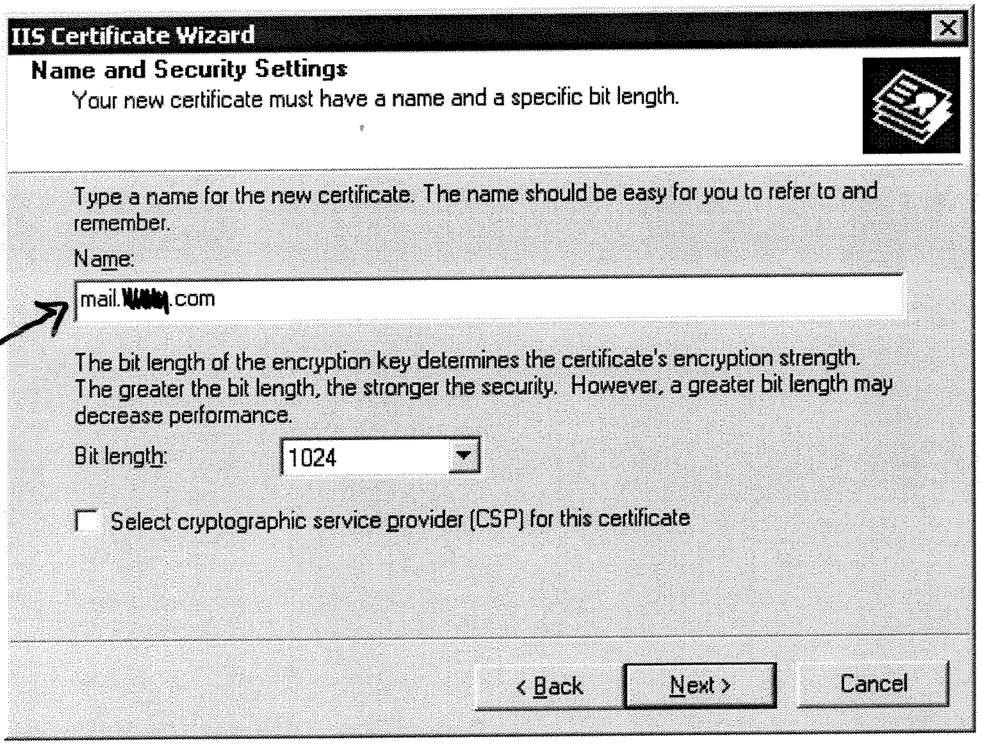
Delayed or Immediate Request

You can prepare a request to be sent later, or you can send one immediately.

Do you want to prepare a certificate request to be sent later, or do you want to send it immediately to an online certification authority?

○ Prepare the request now, but send it later

● Send the request immediately to an online certification authority



Name and Security Settings

Your new certificate must have a name and a specific bit length.

Type a name for the new certificate. The name should be easy for you to refer to and remember.

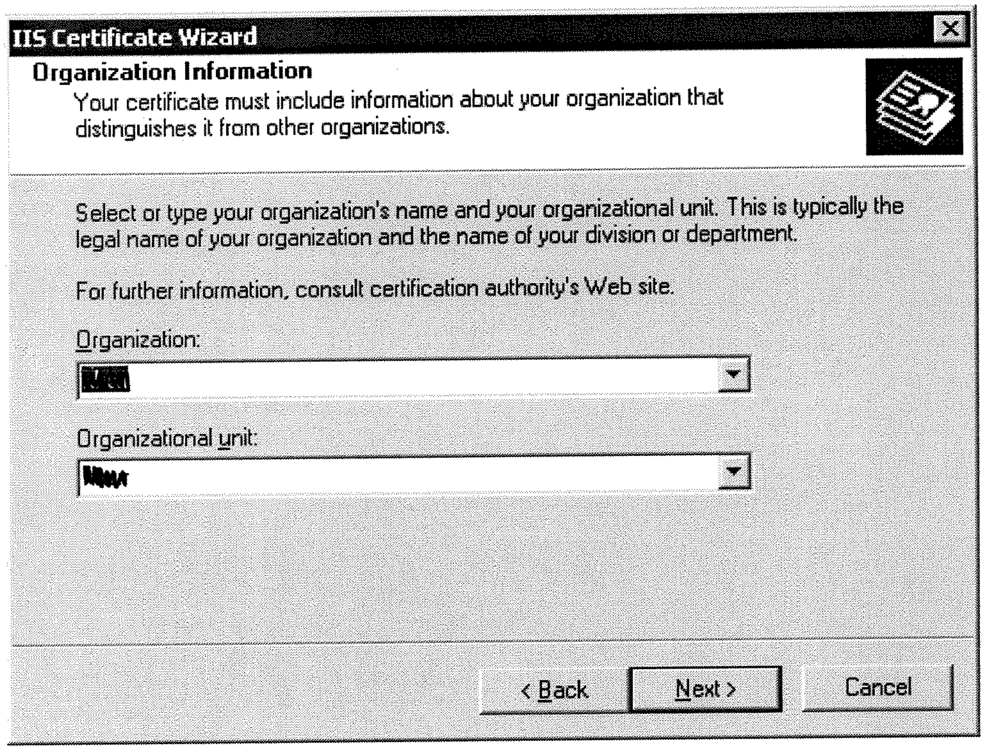
Name: mail.[redacted].com

The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Bit length: 1024

☐ Select cryptographic service provider (CSP) for this certificate

FQDN Here



Organization Information

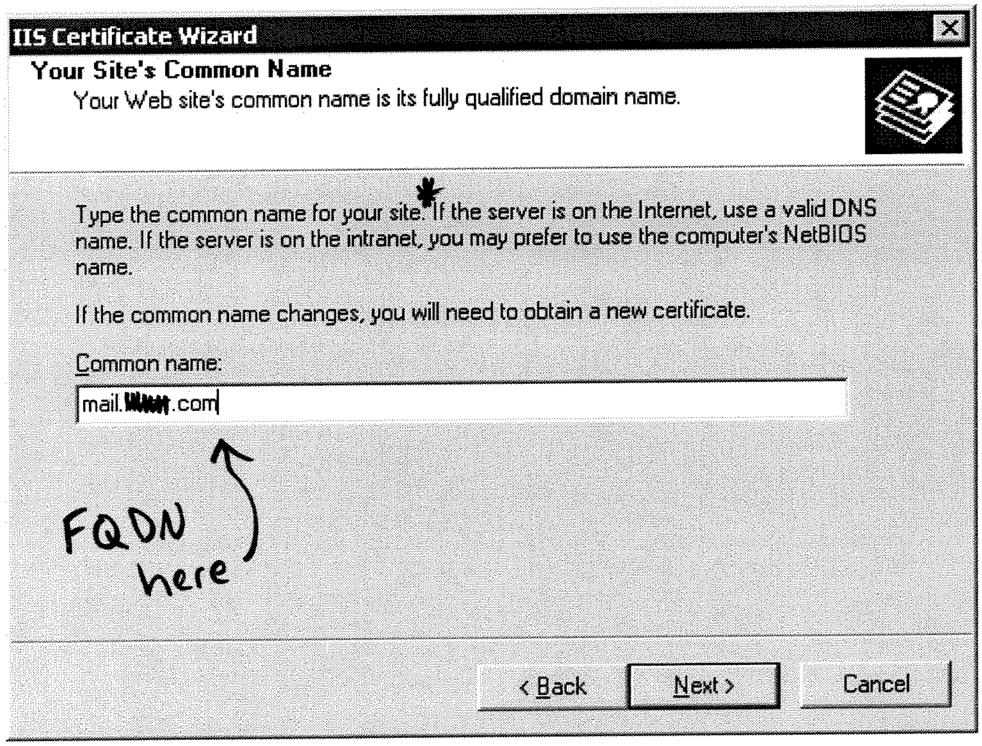
Your certificate must include information about your organization that distinguishes it from other organizations.

Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.

For further information, consult certification authority's Web site.

Organization: [redacted]

Organizational unit: [redacted]



Your Site's Common Name

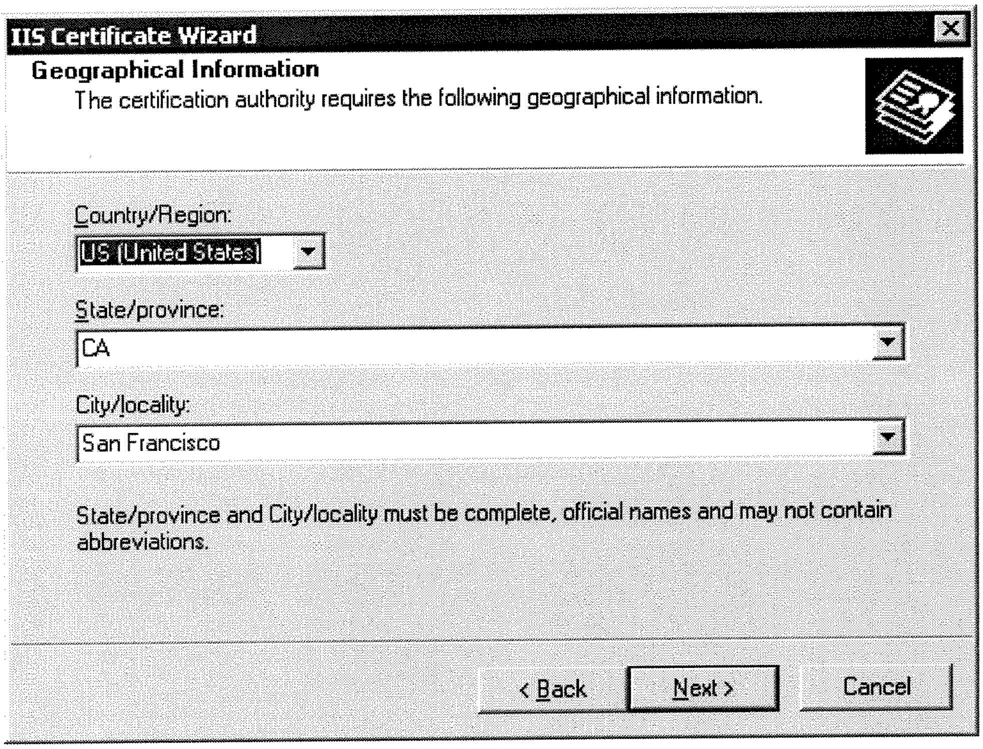
Your Web site's common name is its fully qualified domain name.

Type the common name for your site.* If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name.

If the common name changes, you will need to obtain a new certificate.

Common name: mail.[redacted].com

FQDN here



Geographical Information

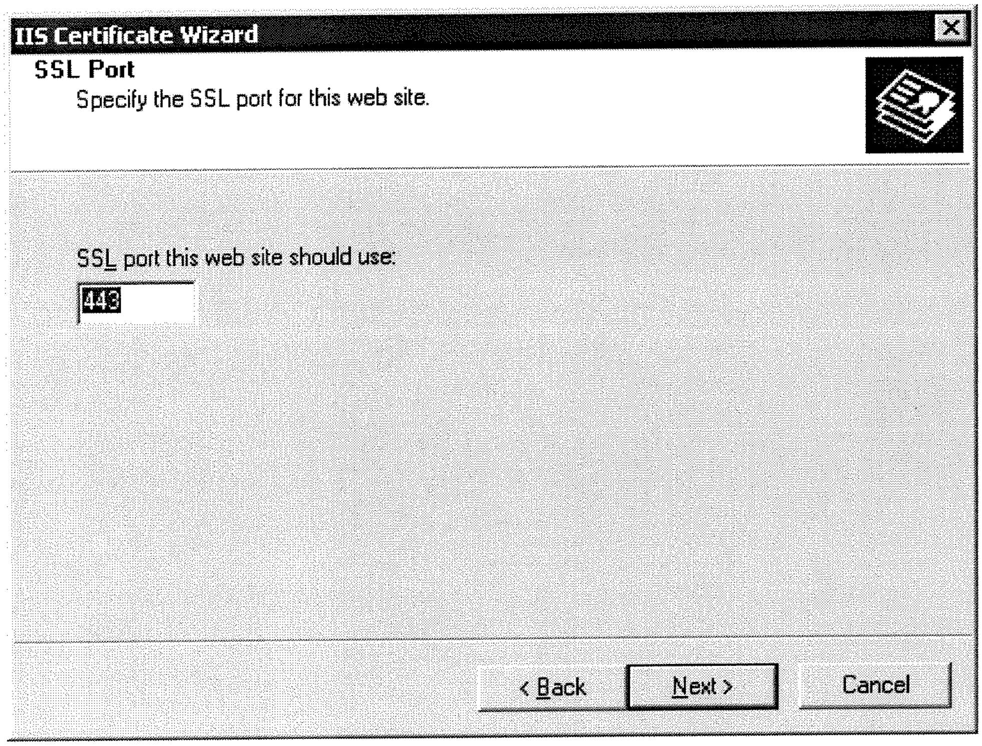
The certification authority requires the following geographical information.

Country/Region: US (United States)

State/province: CA

City/locality: San Francisco

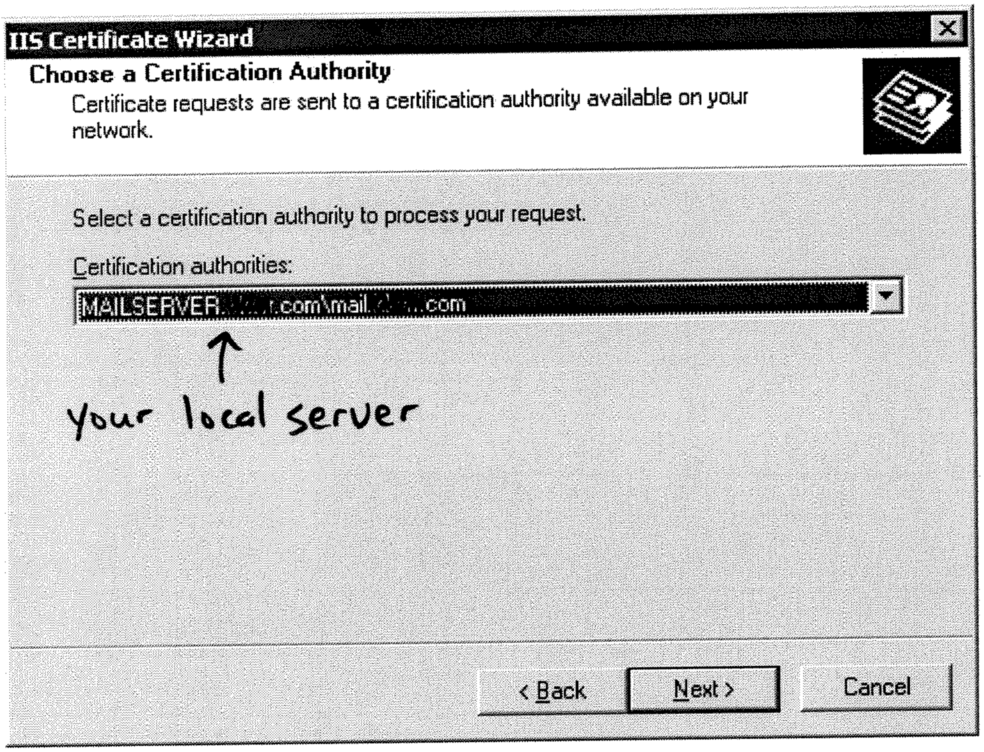
State/province and City/locality must be complete, official names and may not contain abbreviations.



SSL Port

Specify the SSL port for this web site.

SSL port this web site should use: 443



IIS Certificate Wizard

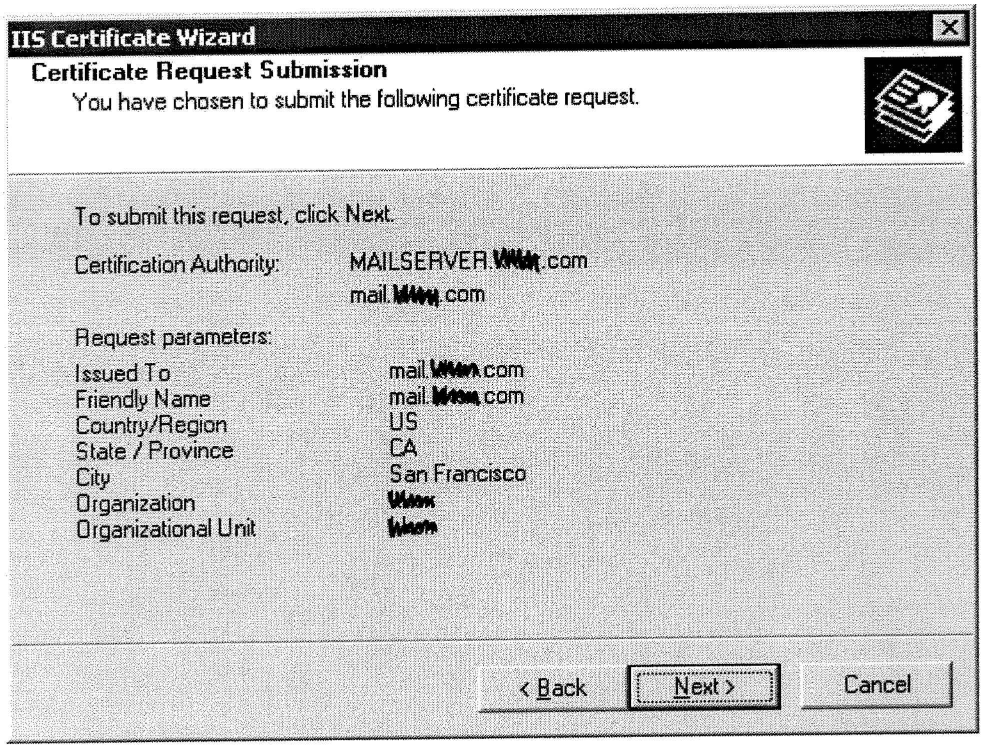
Choose a Certification Authority

Certificate requests are sent to a certification authority available on your network.

Select a certification authority to process your request.

Certification authorities: MAILSERVER.[redacted].com\mail.[redacted].com

your local server



IIS Certificate Wizard

Certificate Request Submission

You have chosen to submit the following certificate request.

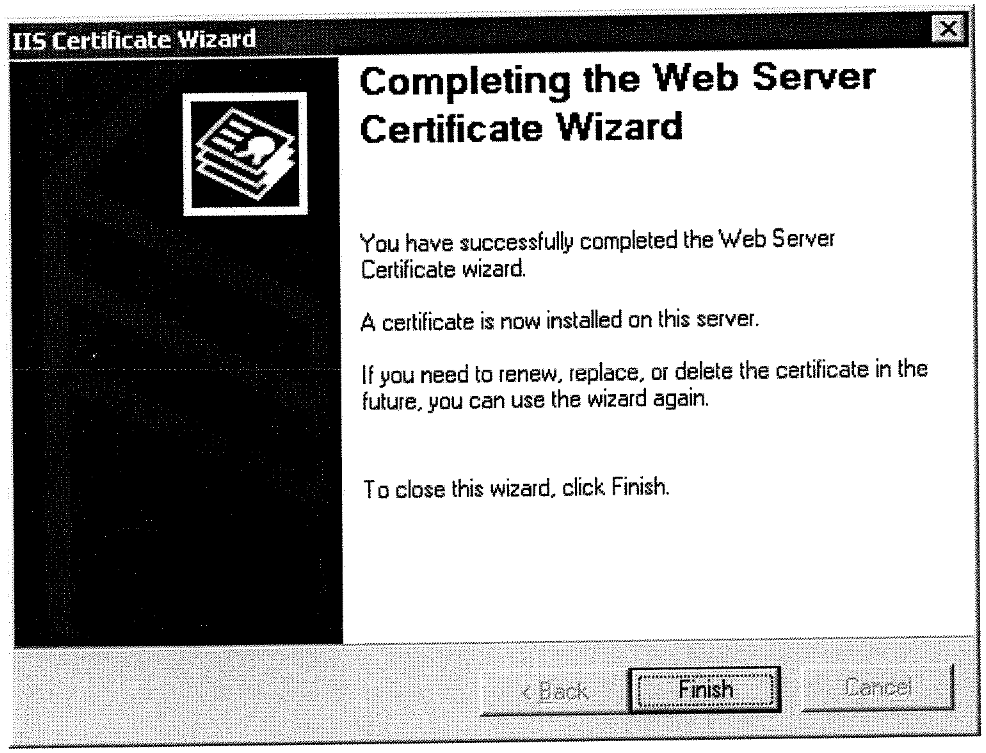
To submit this request, click Next.

Certification Authority: MAILSERVER.[redacted].com
mail.[redacted].com

Request parameters:

Issued To	mail.[redacted].com
Friendly Name	mail.[redacted].com
Country/Region	US
State / Province	CA
City	San Francisco
Organization	[redacted]
Organizational Unit	[redacted]

(24)



Completing the Web Server Certificate Wizard

You have successfully completed the Web Server Certificate wizard.

A certificate is now installed on this server.

If you need to renew, replace, or delete the certificate in the future, you can use the wizard again.

To close this wizard, click Finish.