

# Configure a PKI Using Microsoft® Windows Server™ 2003

If you do not already have a public key infrastructure (PKI) in place within your organization and you would like to take advantage of the SecureZIP features that use digital certificates, here's how to configure the tools for creating a PKI that Microsoft includes with Windows Server 2003.

A *public key infrastructure* is a system to support issuing, using, and managing digital certificates that use public key cryptography to validate and secure electronic transactions.

With a PKI in place, SecureZIP can use digital certificates to strongly encrypt, digitally sign, and authenticate files. You can even attach the files to Microsoft Outlook® email messages directly from SecureZIP.

To make full use of SecureZIP's certificate-based security features with Windows Server 2003, you must first deploy Microsoft Active Directory® or another LDAP-compliant directory service to provide accessible locations for storing certificates, and you must install Certificate Services. Certificate Services enables you to set up an enterprise certification authority from which to request certificates. Certificate Services also helps you manage certificates.

**Note:** To access certificates stored in Active Directory, SecureZIP requires the Directory Integration module, a separately licensed add-on to SecureZIP.

SecureZIP uses certificates stored on an Active Directory server only for encrypting. SecureZIP does not use certificates in a directory to digitally sign files or to authenticate digital signatures.

This brief guide describes how to install Active Directory and Certificate Services on Windows Server 2003, Enterprise Edition, and how to use Certificate Services to set up your own certification authority (CA). Once you have the CA set up, you can begin making certificate requests.

This guide assumes that you have the IIS Web server installed. You must have IIS installed to use the Web enrollment features of Microsoft Certificate Services.

For more comprehensive information about Active Directory and Certificate Services, see the top-level topics “Active Directory” and “Security” on the Microsoft Windows Server 2003 TechCenter Web site:

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/2e0186ba-1a09-42b5-81c8-3ecca4ddde5e.mspx>

Contents

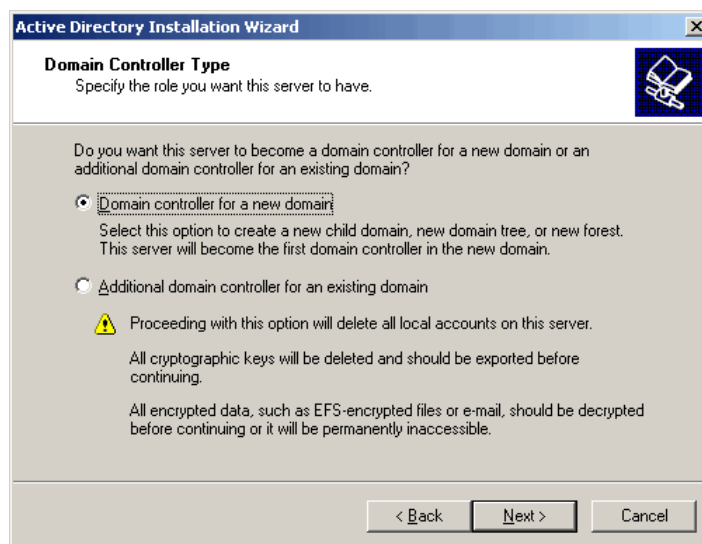
- Configure a PKI Using Microsoft® Windows Server™ 2003..... 1**
  - Install Microsoft Active Directory ..... 4*
  - Install Certificate Services as an Enterprise Root Certification Authority..... 9*
- Request and Install User Certificates ..... 14**
  - Use the Web Enrollment Form ..... 14*
  - Use the Certificate Management Console..... 17*
- Configure SecureZIP for Windows To Access Your Certificates ..... 21**
  - Point SecureZIP to Active Directory Certificate Stores ..... 21*
  - Specify Default Certificates in SecureZIP ..... 23*
  - Turn On Encryption and/or Signing in SecureZIP ..... 24*

## Install Microsoft Active Directory

The following steps describe how to install Active Directory on Windows Server 2003, Enterprise Edition. Active Directory provides a place to keep the public key portion of a certificate where it can be accessed for asymmetric encryption. Your personal certificate(s) with their private keys are installed on your own machine.

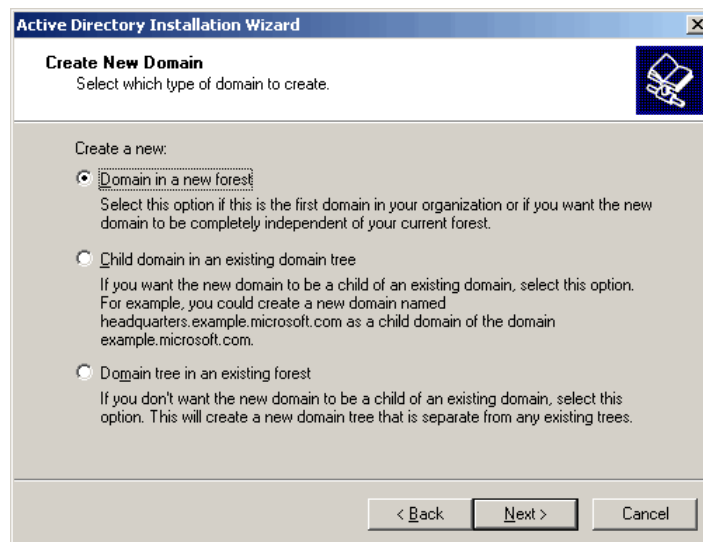
The steps below describe how to install Active Directory in a new domain.

1. Log in to the Windows 2003 server that you want to make the domain controller for a new domain.
2. Open the Active Directory Installation wizard: From the Start menu, select **Run**. Type: dcpromo. Click **OK**.

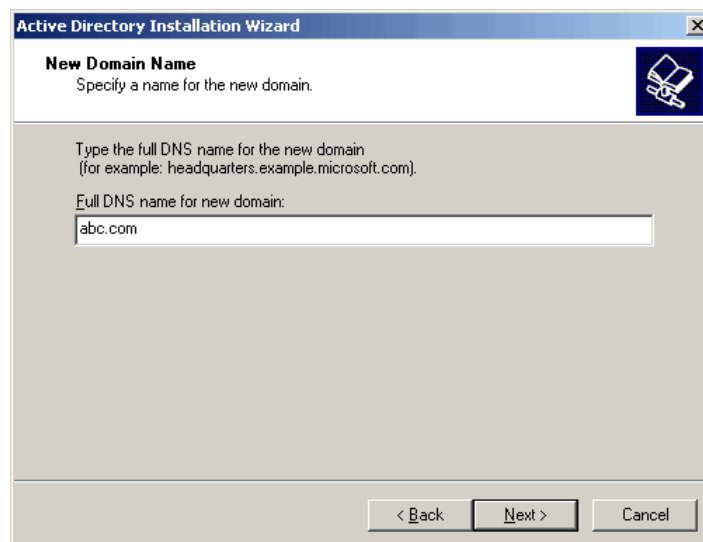


3. Select the option *Domain controller for a new domain*, as shown above, and choose **Next**.

A dialog opens in which to select a type of domain.

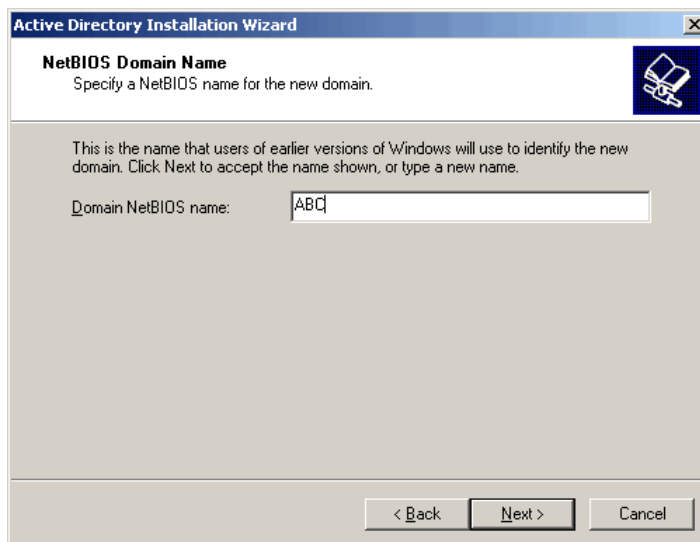


4. Select *Domain in a new forest*, as shown above, and choose **Next**. This opens a dialog in which to specify a name for the new domain.



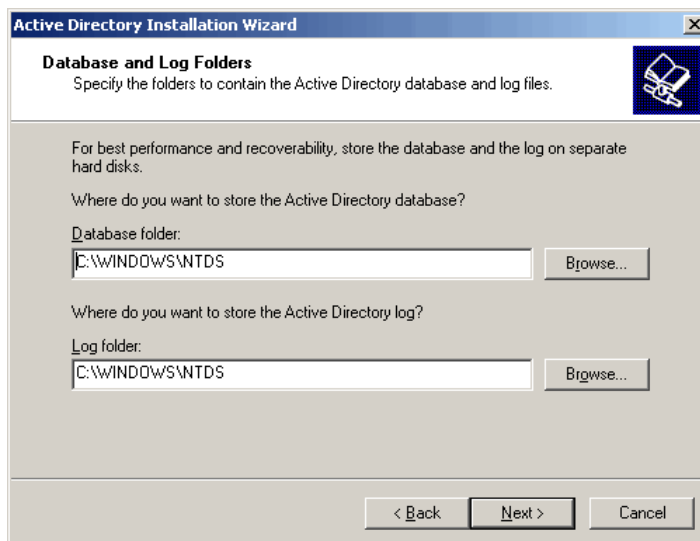
5. Enter a name for the domain. Microsoft recommends using `.local` or `.dom` for internal domains, but you may use any domain name you like. Choose **Next**.

A dialog opens in which to specify a NetBIOS name for the domain.

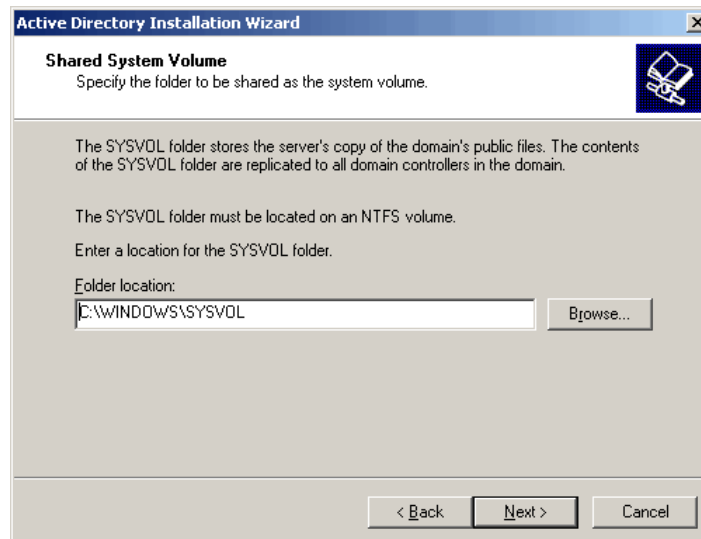


6. Accept the proposed NetBIOS name or enter a different one and choose **Next**.

A dialog opens in which to specify folder locations for the Active Directory database and log files.

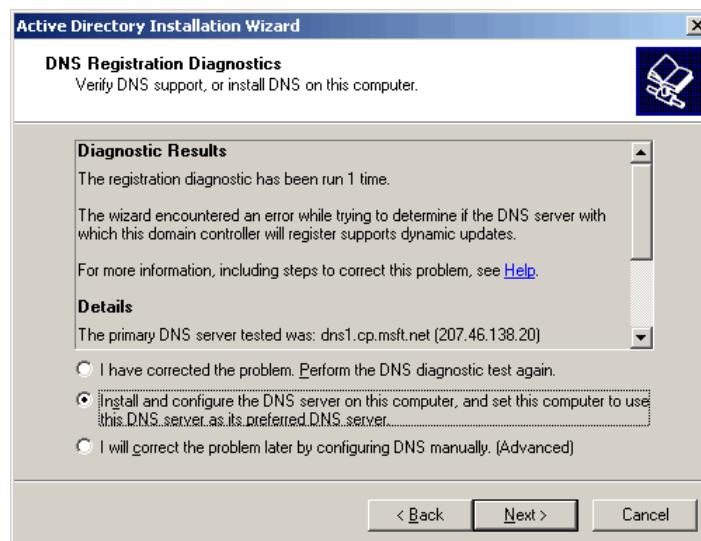


7. Select locations for the Active Directory database and log file. Choose **Next** to open a dialog in which to specify a folder to be shared as the system volume.



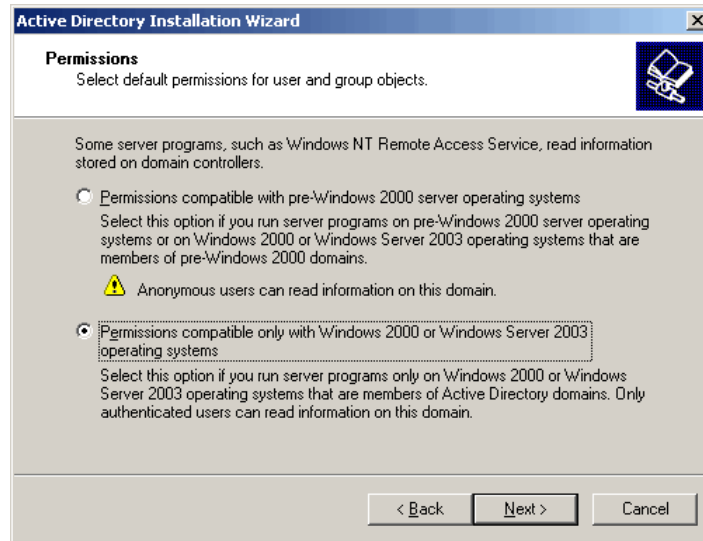
8. Specify a location for the shared system volume and choose **Next**.

The following dialog appears if DNS is not already installed on the local computer.



To install DNS, select *Install and configure the DNS server...*, as shown in the screenshot above, and choose **Next**.

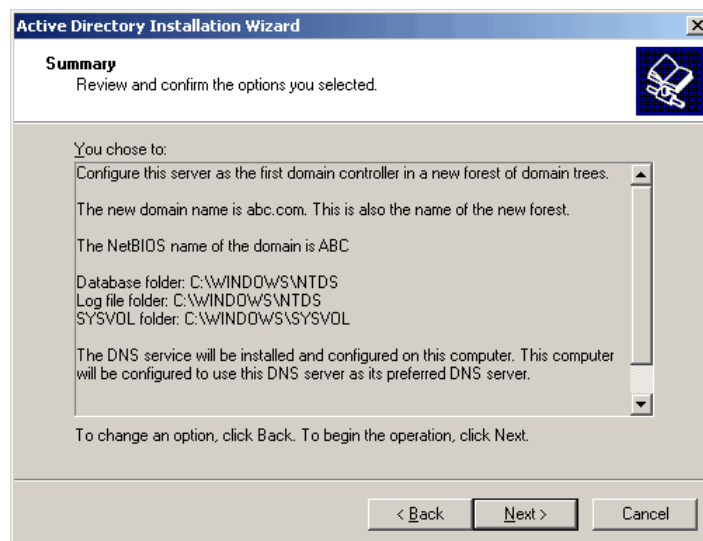
A dialog opens in which to specify the type of permissions you want Active Directory to use.



9. Select whether to install Active Directory to use permissions compatible with pre-Windows 2000 operating systems (mixed mode) or permissions compatible only with Windows 2000 or Windows Server 2003 operating systems (native mode).

Mixed mode supports pre-Windows 2000 domain controllers; native mode does not. Native mode is preferable if you do not need to support programs running on pre-Windows 2000 operating systems.

Choose **Next** to display a summary of your settings.





**10. Choose **Next** to install Active Directory.**

After Active Directory is installed, you are prompted to reboot. You can then log in to the domain. At this point, you can configure workstations to join and log in to the domain.

For clients to find the new domain, you must update any lookup zones on your internal DNS servers to point to the new domain controller. Alternatively, you may point clients to the new domain controller for DNS. If clients require Internet name resolution, you will need to configure this on the forwarder's tab on the new domain controller's internal DNS server.

For more information about working with a DNS server, see the topic, "DNS server role: Configuring a DNS server," on the Microsoft Windows Server 2003 TechCenter Web site:

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/4e1c7b17-16ab-4e7d-a333-15befb15c82e.mspx>

## Install Certificate Services as an Enterprise Root Certification Authority

The following steps describe how to install Certificate Services on Windows Server 2003, Enterprise Edition, and how to set up an enterprise root certification authority. Certificate Services enables you to request and manage certificates.

These steps assume that Active Directory is already deployed.

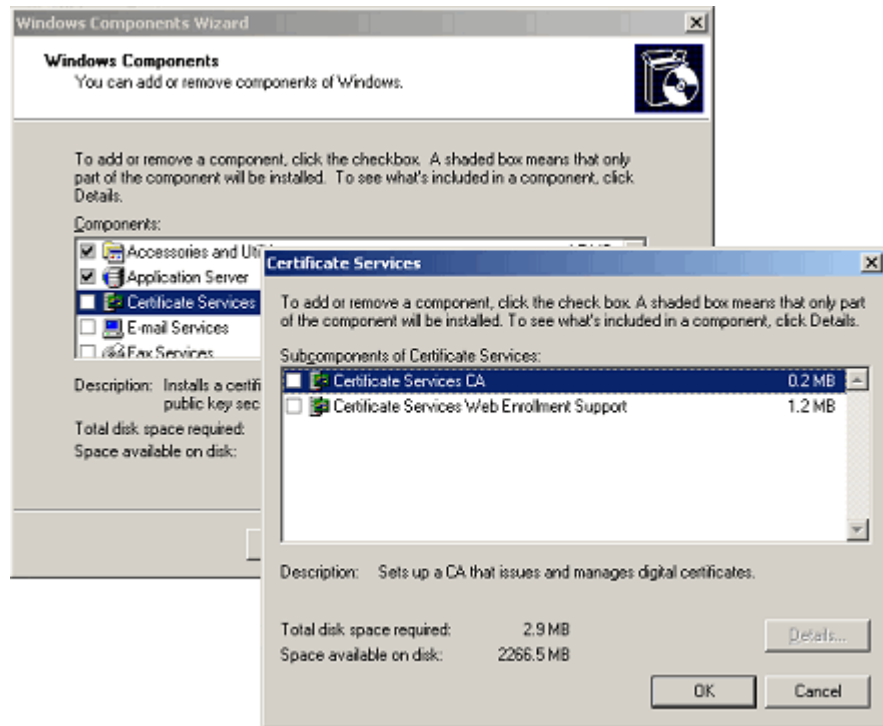
1. Log in to a domain controller or member server with an account that is a member of both the Enterprise Admins group and the Domain Admins group.

**Note:** If your organization has, or has ever had, any Windows 2000 Certificate Authorities, you must install the new Windows 2003 certificate templates before proceeding. See "Install new templates and upgrade existing templates" on the Microsoft Windows Server 2003 TechCenter Web site:

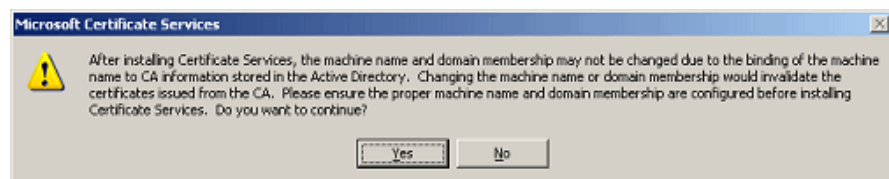
<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/9944aee5-cd81-4f4a-8e4c-109e913a0d79.mspx>

2. Open the Add/Remove Programs application in the Control Panel.

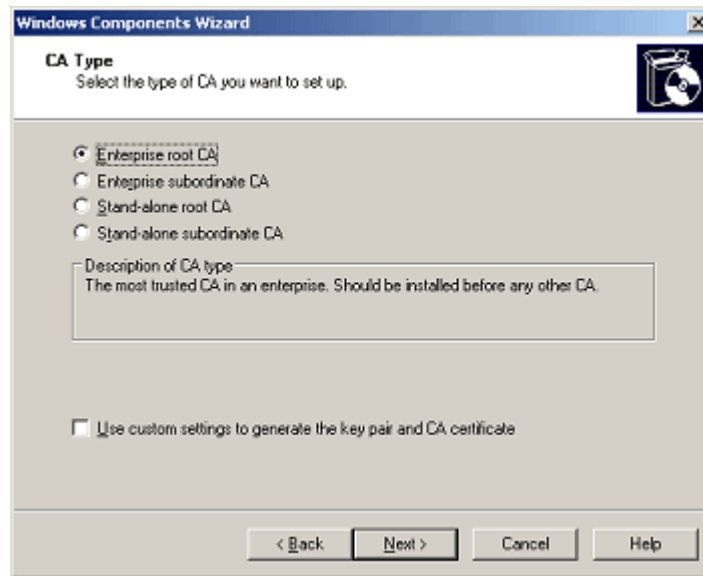
3. Select **Add/Remove Windows Components**.
4. In the Windows Components wizard, highlight *Certificate Services* and choose **Details**. Select both the *Certificate Services CA* and *Web Enrollment Support*. Choose **OK**.



A dialog appears with a note cautioning that the local machine name and domain membership will be bound to the CA information.



5. Choose **Yes**. A dialog opens in which to select the type of certification authority to set up.



6. Select *Enterprise Root CA*.

Installing an enterprise root CA allows all computers that are members of the target domain to automatically trust the CA.

If you know how to configure a CA, you can alternatively select a stand-alone root or subordinate CA. SecureZIP works with either of these as well.

Choose **Next** to open a dialog in which to define the CA.

The screenshot shows the 'CA Identifying Information' dialog box in the Windows Components Wizard. The title bar reads 'Windows Components Wizard'. The main heading is 'CA Identifying Information' with the instruction 'Enter information to identify this CA.' Below this, there are three text input fields: 'Common name for this CA:' containing 'ABC Corp CA', 'Distinguished name suffix:' containing 'DC=abc,DC=com', and 'Preview of distinguished name:' containing 'CN=ABC Corp CA,DC=abc,DC=com'. At the bottom left, there is a 'Validity period:' section with a dropdown set to '5' and 'Years'. To the right, the 'Expiration date:' is '5/17/2010 11:22 AM'. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

7. Specify a name and validity period for the CA. Choose **Next**.

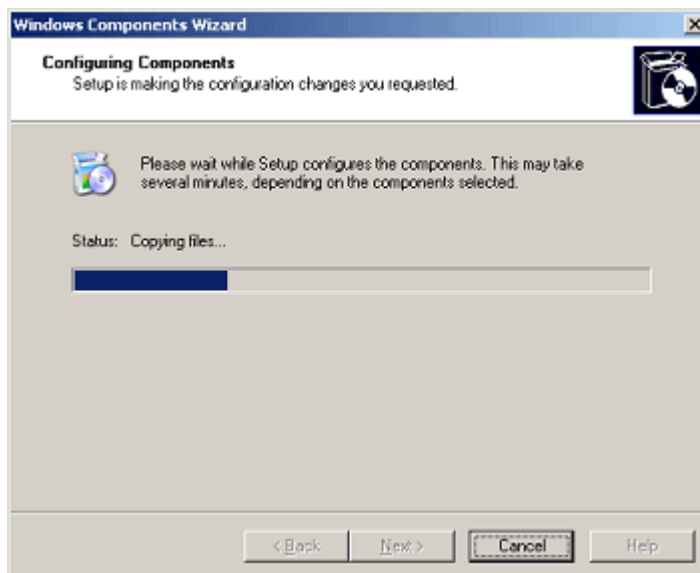
A dialog opens in which to enter locations for the certificate database and log.

The screenshot shows the 'Certificate Database Settings' dialog box in the Windows Components Wizard. The title bar reads 'Windows Components Wizard'. The main heading is 'Certificate Database Settings' with the instruction 'Enter locations for the certificate database, database log, and configuration information.' Below this, there are two text input fields: 'Certificate database:' containing 'C:\WINDOWS\system32\CertLog' and 'Certificate database log:' containing 'C:\WINDOWS\system32\CertLog'. Each field has a 'Browse...' button to its right. Below these, there is a checkbox labeled 'Store configuration information in a shared folder'. If checked, there would be a 'Shared folder:' text input field and a 'Browse...' button. At the bottom, there is another checkbox labeled 'Preserve existing certificate database'. At the very bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

8. Specify the locations for the certificate database, database log, and the shared folder (defaults are acceptable). Choose: **Next**.

If IIS is running, a prompt informs that it needs to be restarted. Choose **OK**.

Setup now completes. You may be required to insert your Windows 2003 Server installation media or to point the installer to a .cab file on the network.



## Request and Install User Certificates

Now that Certificate Services is installed and ready to use, users can request certificates from the enterprise certification authority (CA) set up in the preceding steps.

Users can request certificates in two ways:

- Using the CA's Web enrollment form
- Using the Certificate Management console

Both methods install the requested certificates private key into the logged-in user's personal store. If the CA has been configured as an enterprise CA, the CA automatically publishes keys into Active Directory.

Both methods install the requested certificate with its private key on the local Windows computer and publish the certificate's public key to Active Directory.

### Use the Web Enrollment Form

Users can enroll for personal certificates through the Certificate Services Web enrollment form located at the URL:

`http://servername/CertSrv`

where *servername* is the name of the Web server running Windows Server 2003 where the CA you want to access is located.

The following steps show a straightforward way to request a user certificate through Web enrollment. As the accompanying screens indicate, the process can be customized in various ways.

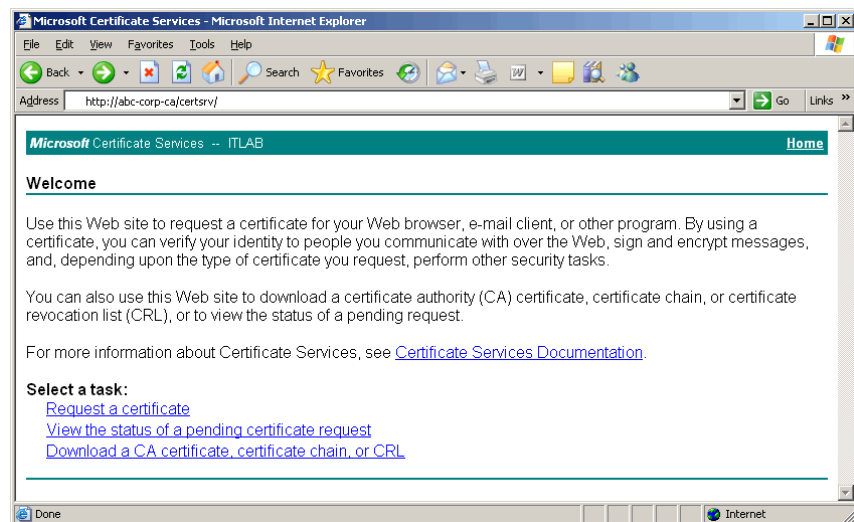
For detailed instructions on requesting certificates over the Web, see the topic, "Submit a user certificate request via the Web to a Windows Server 2003 CA," on the Microsoft Windows Server 2003 TechCenter Web site, here:

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/b105bc5d-db4a-4570-90f1-873819d3a5cf.mspx>

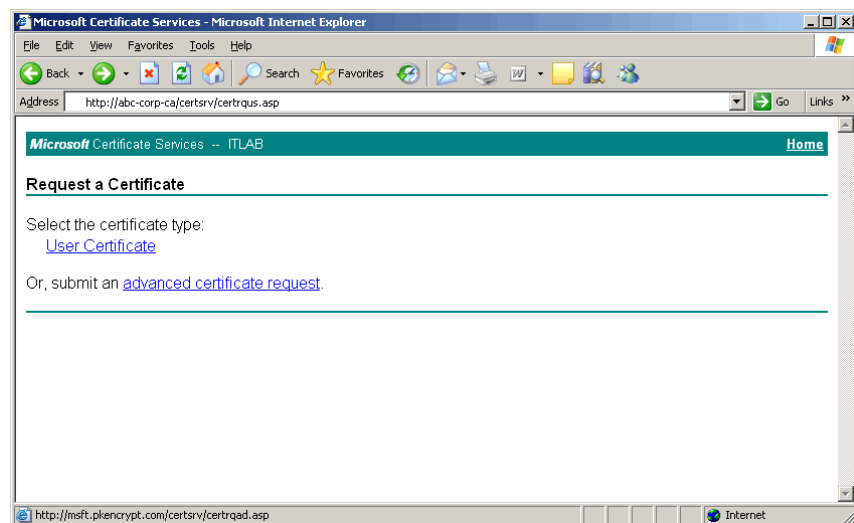
The TechCenter Web site also contains a wealth of information on administering a CA and on managing certificates.

To use Web enrollment to request a user certificate:

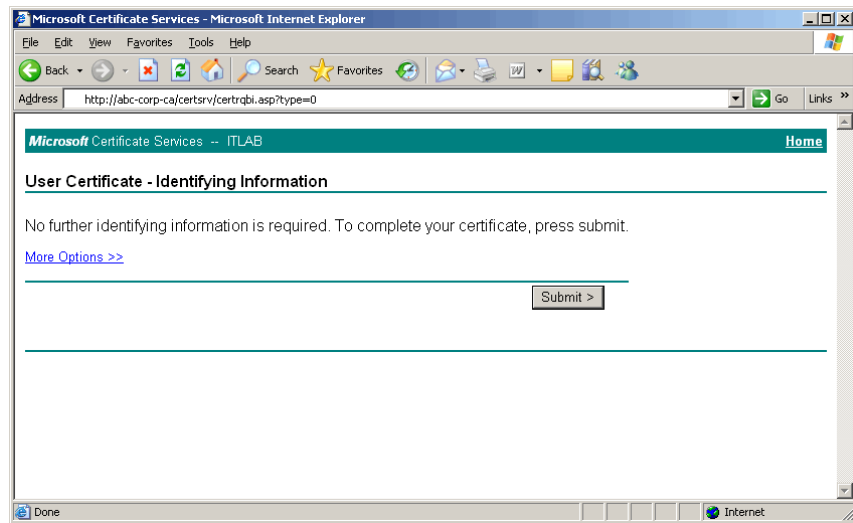
1. In your Internet Explorer browser, navigate to the URL of the Web form for the CA from which you want to request a user certificate. For example, for a CA located on Web server abc-corp-ca, navigate to:  
`http://abc-corp-ca/certsrv/`



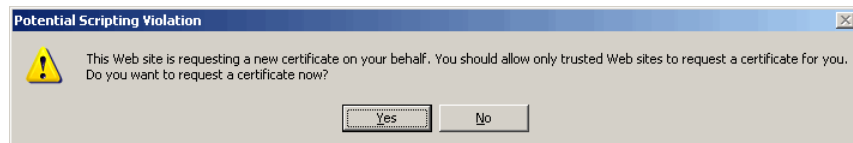
2. On the Welcome screen shown above, choose the link, *Request a certificate*, to open the page shown below.



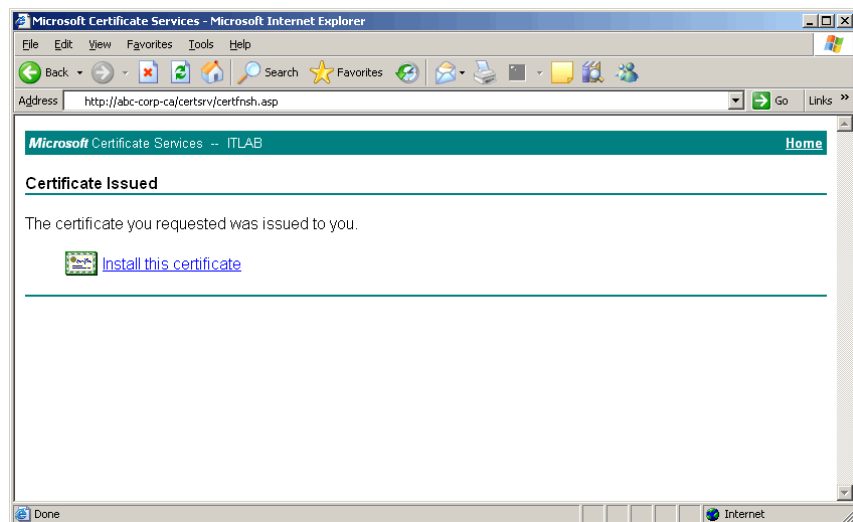
3. Choose the link, *User Certificate*, to open the page shown below.



4. Choose the **Submit** button to submit your request. The following message displays.



5. Choose **Yes** to complete your request. The following confirmation screen displays.



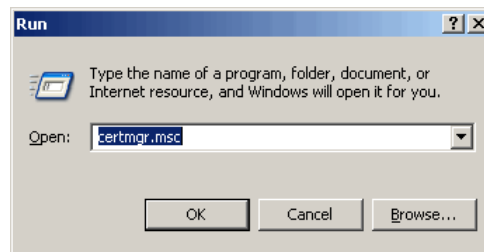


6. Choose *Install this certificate* to install the certificate with its private key on the local machine and to publish the public key to Active Directory where it can be accessed by other users.

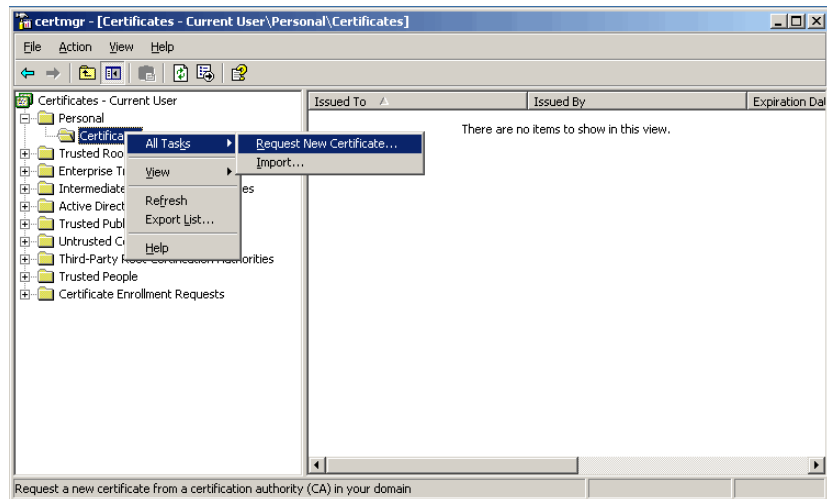
## Use the Certificate Management Console

As an alternative to requesting a certificate through a CA's Web enrollment form, as described above, users can use the Certificate Management console to request a certificate from an enterprise root CA. The Certificate Management console is a Microsoft Management Console (MMC) snap-in that is included with NT 5.0 and later versions of Windows. It uses LDAP to query PKI information from a local domain controller.

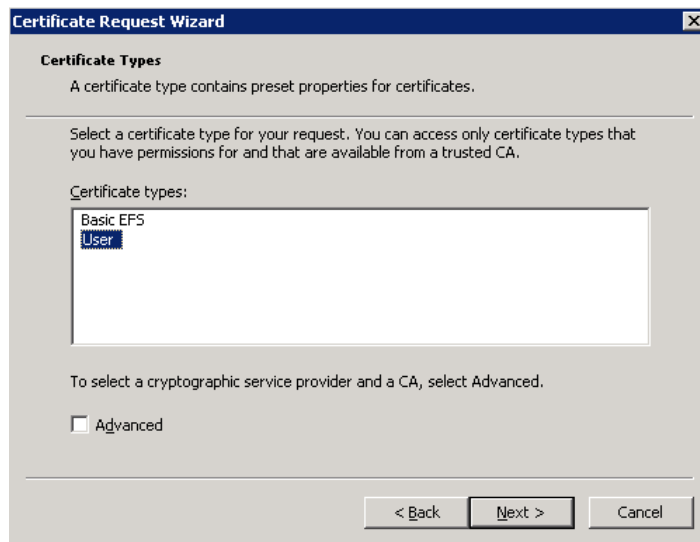
1. Open the Certificate Management console (certmgr): From the Start menu, choose **Run....** Enter `certmgr.msc`, as shown below, and choose **OK**.



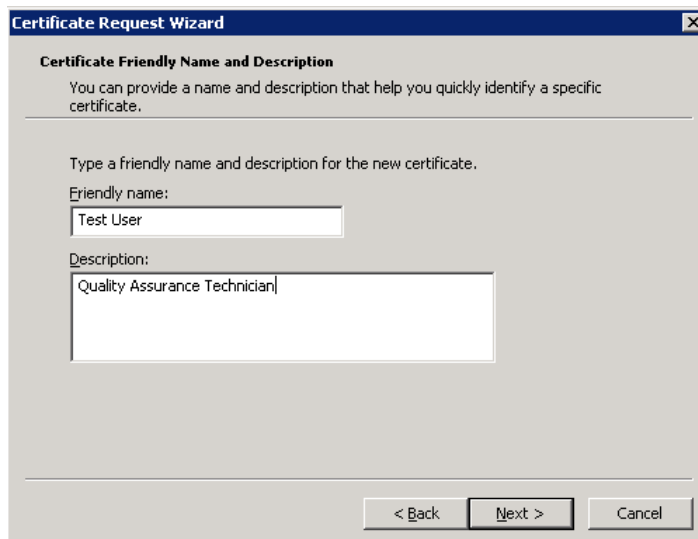
2. Run the Certificate Request wizard: In the certmgr console, expand the Personal folder in the console tree (lefthand pane). Right click the Certificates folder to open the context menu. Choose **All Tasks | Request New Certificate...**, as shown below.



3. In the Certificate Request wizard, select the type of certificate you want to request: Select *User*, as shown below, and choose **Next**.



4. As shown below, enter a friendly name and description that will help you identify the certificate. Choose **Next**.



The screenshot shows the 'Certificate Request Wizard' window, specifically the 'Certificate Friendly Name and Description' step. The window title is 'Certificate Request Wizard'. The main heading is 'Certificate Friendly Name and Description'. Below this, a message states: 'You can provide a name and description that help you quickly identify a specific certificate.' A sub-instruction says: 'Type a friendly name and description for the new certificate.' There are two input fields: 'Friendly name:' with the text 'Test User' and 'Description:' with the text 'Quality Assurance Technician'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

5. In the final wizard screen, review your settings. If they are okay, choose **Finish** to complete the wizard.

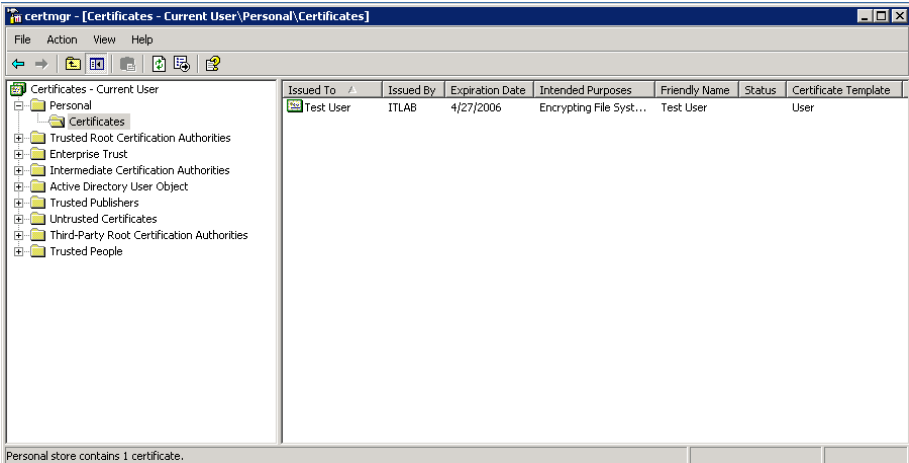


The screenshot shows the 'Certificate Request Wizard' window at the final step, 'Completing the Certificate Request Wizard'. The window title is 'Certificate Request Wizard'. On the left, there is a graphic of a certificate. The main heading is 'Completing the Certificate Request Wizard'. Below this, a message states: 'You have successfully completed the Certificate Request wizard.' Another message says: 'You have specified the following settings:'. Below this is a table showing the settings:

Friendly Name	Test User
Account Name	Test_User
Computer Name	ABCCORP
Certificate Template	User

At the bottom right, there are three buttons: '< Back', 'Finish', and 'Cancel'.

- 6. Check in the Certificate Management console to confirm that your certificate has been issued and installed in your personal certificate store.



## Configure *SecureZIP* for Windows To Access Your Certificates

To configure SecureZIP for Windows to use certificates for encryption/decryption and for working with digital signatures, you must do these things in SecureZIP:

- Add the Active Directory certificate store(s) to the list of stores that SecureZIP checks for certificates
- Have each user designate a default certificate to use when he does certificate-based encryption
- Turn on encryption or signing in SecureZIP to have SecureZIP encrypt or sign files

### Point SecureZIP to Active Directory Certificate Stores

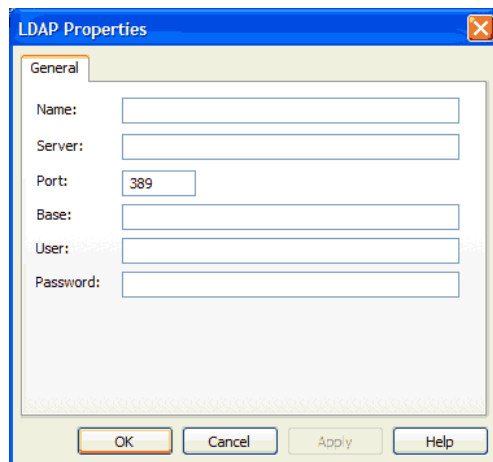
For SecureZIP for Windows to access your Active Directory certificates to encrypt for the certificates' owners, you must tell SecureZIP where the certificates are.

To do this, open SecureZIP and do the following:

1. In the Tools menu, select **Options...** to open the SecureZIP Options dialog.
2. Select the Security category.
3. Select the Certificate Stores tab to see a list of certificate stores SecureZIP can search..

The Certificate Stores list contains an item for every certificate store SecureZIP knows about. A store is labeled either *Local* or *LDAP* in the Type column, depending on whether the store is on your local system or on an LDAP-compliant directory server such as Active Directory. LDAP is a protocol used by Active Directory and other directory servers.

4. Choose the **Add...** button to open a new LDAP Properties page.



The screenshot shows the 'LDAP Properties' dialog box with the 'General' tab selected. The dialog has a title bar with a close button. Inside, there are several text input fields: 'Name:', 'Server:', 'Port:' (containing '389'), 'Base:', 'User:', and 'Password:'. At the bottom, there are four buttons: 'OK', 'Cancel', 'Apply', and 'Help'.

5. In the LDAP Properties dialog, fill in the fields with the information SecureZIP needs to access the directory. When done, choose **OK** to return to the Certificate Stores tab.

The fields in the LDAP Properties dialog are described in the following table. The fields marked *Optional* may be left blank unless they are required to access the server. Only the Name and Base fields are required.

<b>Field</b>	<b>Description</b>
<b>Name</b>	A label to identify the server in the Certificate Stores list. For example: Gamma
<b>Server</b>	(Optional) The TCP/IP address of the LDAP server or a name that resolves to such an address. For example: 192.172.0.1
<b>Port</b>	(Optional) The TCP/IP port to use. Port 389 is customary and is entered as the default.
<b>Base</b>	<p>The name of the entry that SecureZIP should use as the base or root of the LDAP search for certificates, analogous to a root folder or directory in a file system. For example: cn=users,dc=xyz,dc=com</p> <p>The query string format for the LDAP base can vary between LDAP implementations. For example, a server may expect query strings in the Internet domain-style format used by default by Microsoft Active Directory (for example, cn=users,dc=xyz,dc=com), or it may expect them in X.500 naming format (for example, o=xyz,c=US). Check with your LDAP or network administrator for the query string to use.</p>
<b>User</b>	(Optional) The user account with which to log in if the LDAP server requires a login
<b>Password</b>	(Optional) The password associated with the user account

6. On the Certificates Stores tab, choose **OK** or **Apply...** to save the new certificate store for SecureZIP to use.

## Specify Default Certificates in SecureZIP

Users may have one or more personal certificates that they use to sign files or to ensure that they can decrypt files that they encrypt for others. If a user has only one certificate, SecureZIP automatically uses that certificate. If a user has more than one, the user can tell SecureZIP which certificate to use by default.

To specify a default certificate to use when encrypting for yourself:

1. In SecureZIP, in the Tools menu, select **Options...** to open the SecureZIP Options dialog.
2. Select the Security category.
3. Select the Encryption tab.

4. In the Method dropdown, select one of the two *Recipient list* options to enable the list of personal certificates.

In the list, a valid certificate displays with a green check mark; an invalid certificate shows a red "X".

5. Select a certificate to use by default.

If you have only one, it is used automatically.

To specify a default certificate to use when signing:

1. In SecureZIP, in the Tools menu, select **Options...** to open the SecureZIP Options dialog.
2. Select the Security category.
3. Select the Authentication tab.
4. Select a certificate to use by default from the list of your personal certificates.

If you have only one certificate, it is used automatically. A valid certificate displays with a green check mark; an invalid certificate shows a red "X".

## Turn On Encryption and/or Signing in SecureZIP

To use certificates to encrypt or sign files in SecureZIP, those functions must be turned on. SecureZIP then routinely encrypts and/or signs files until you turn the functions off.

By default, encryption is turned on and signing is turned off.

To turn on certificate-based encryption:

1. On the Encryption tab of Security Options, in the Method dropdown list, select one of the following:
  - o Strong: Recipient List
  - o Strong: Recipient List or Password
2. Check the box *Encrypt files*.

See the SecureZIP help for other, more direct ways to turn on encryption.



To turn on signing, choose **Sign Files on/off** from the Actions menu. Again, there are other, more direct ways.

SecureZIP is now set up to do certificate-based encryption and apply digital signatures.