

Configuring a Windows 2003 Server for IAS

When setting up a Windows 2003 server to function as an IAS server for our demo environment we will need the server to serve several functions. First of all we will configure the server to be a Domain Controller so that we can use Active Directory to define users and/or machines. Next we will configure the server to act as a Certificate Authority for providing certificate services for our demo environment. In order for the certificate services to operate fully, we will also need to enable IIS to all web access for certificate requests. Finally we need to enable IAS to allow the server to function as a Radius server.

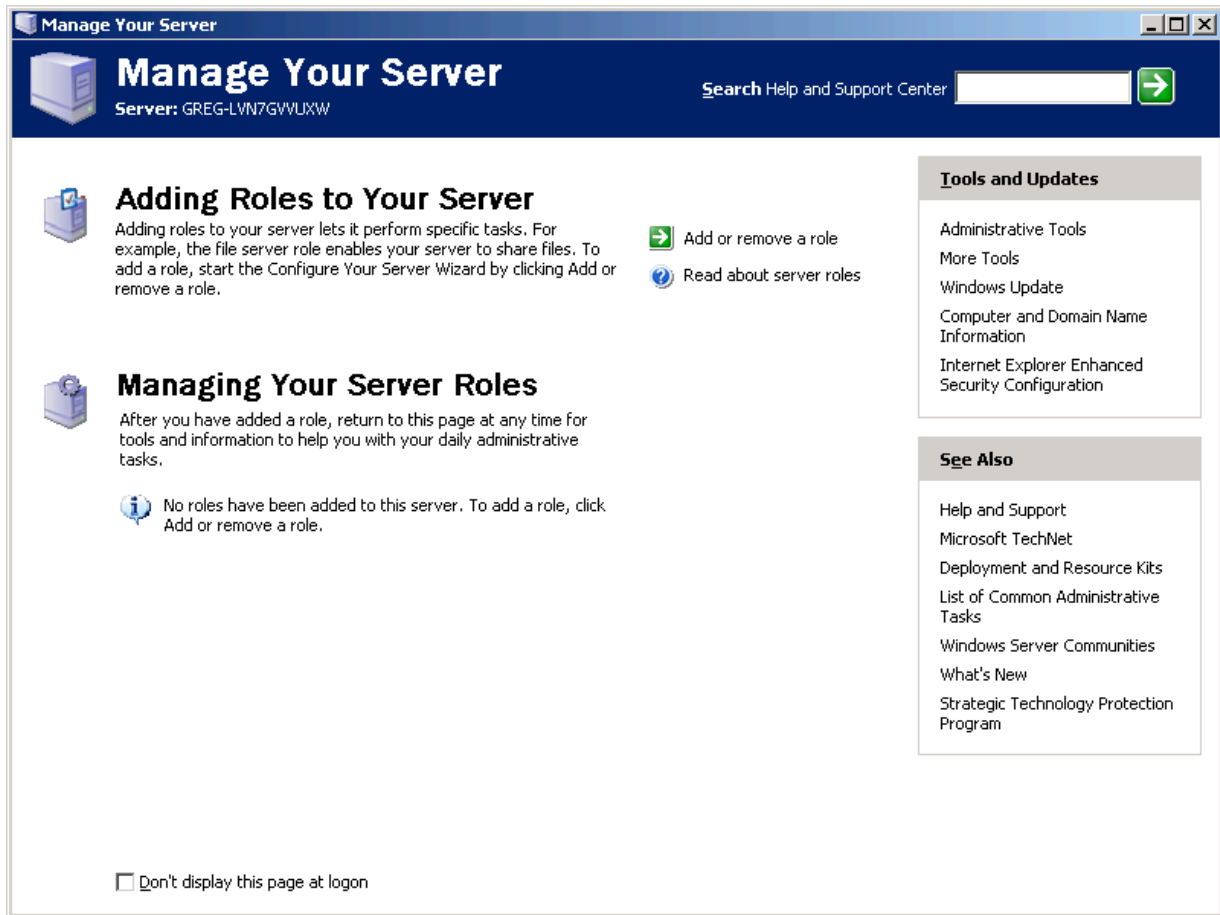
The following tasks should be done in the order shown.

- 1. Configure the Server as a Domain Controller**
- 2. Enable IIS on the Server**
- 3. Configure the Server as a Certificate Authority**
- 4. Download the CA Certificate**
- 5. Enable and configure IAS**

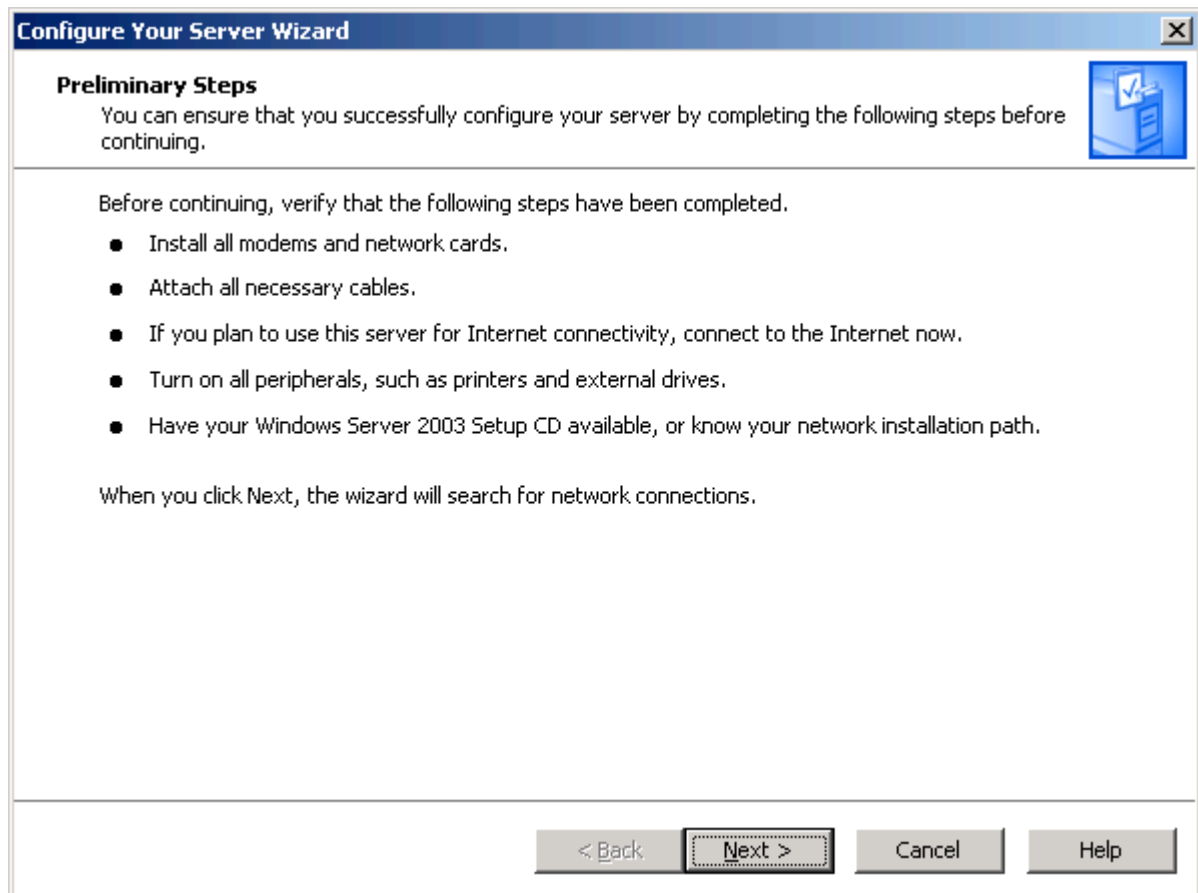
The remainder of this document will show the step by step process required to complete each of these tasks. It is assumed that we will be starting from a freshly installed Windows 2003 Server.

Configure the Server as a Domain Controller

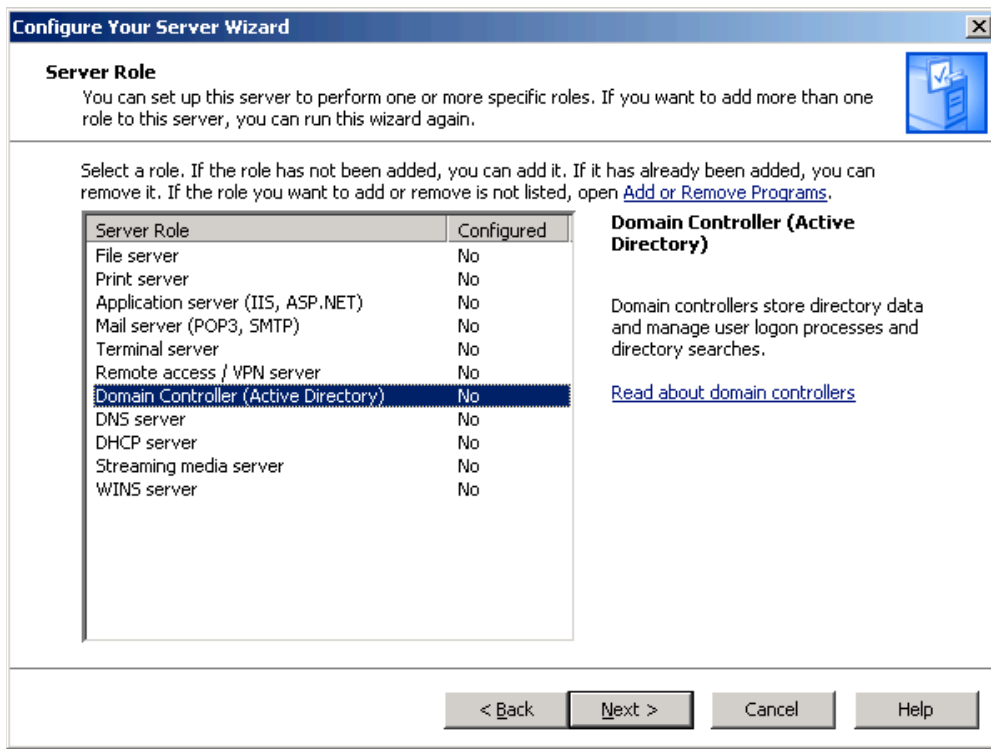
When a newly installed 2003 server is first logged into, the following window will be opened. This Manage Your Server window will allow you to change the role that your server plays on the network. In order to configure the server to be a Domain Controller we need to start the process by selecting the Add or remove a role option in this window.



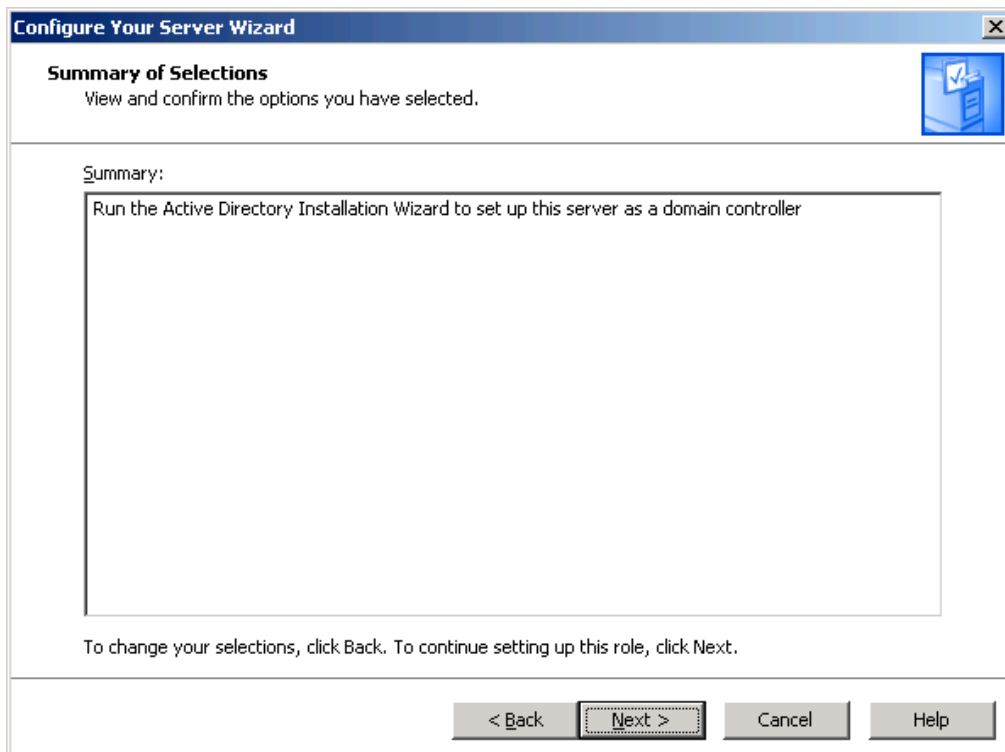
The configuration wizard will now start and ask you to verify that preliminary steps have been completed. Hit “Next” to continue.



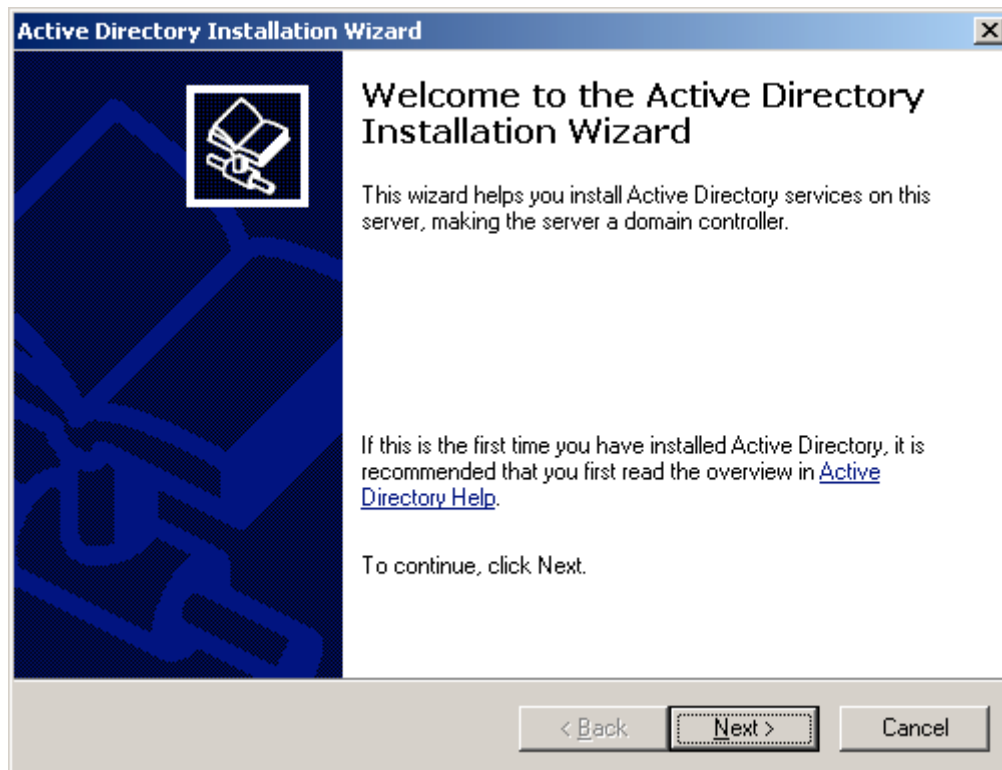
The wizard will then provide a list of server roles that can be configured. As shown below, select “Domain Controller” from the list and hit the “Next” Button.



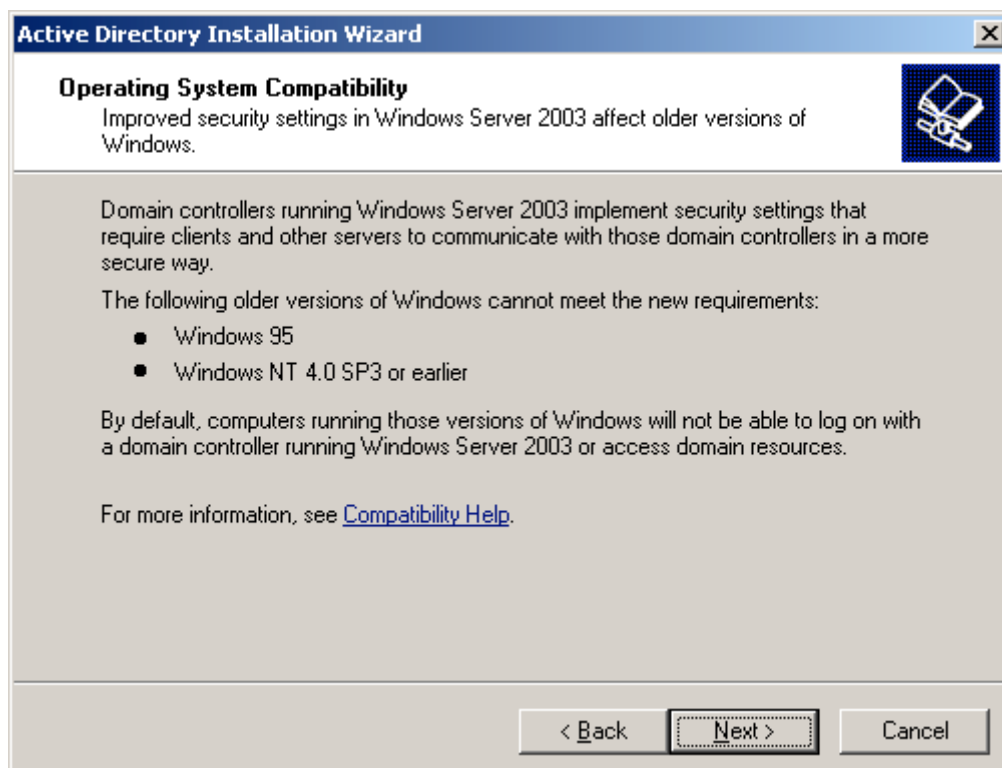
The Wizard will ask you to confirm your selection. Press “Next” to confirm and continue.



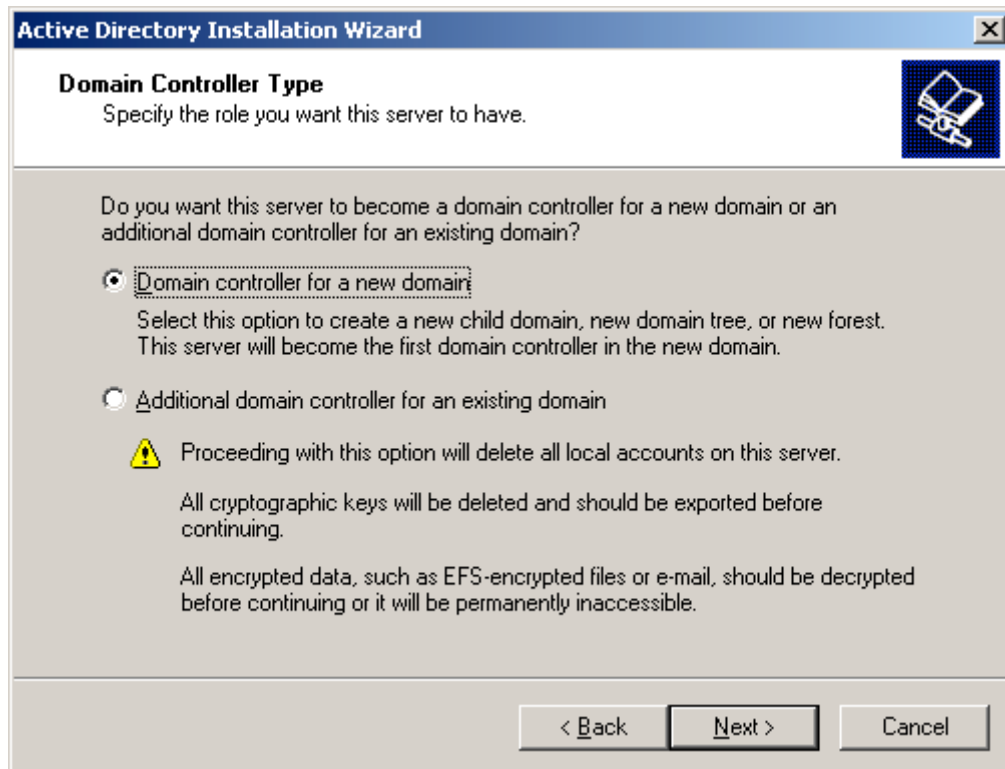
The Active Directory Installation Wizard will now start. Select “Next” to continue.



A warning window will now be displayed. Press “Next” to continue.



You will now be asked to specify a Domain Controller Type. Here we will want to select the Domain controller for a new domain radio button, and select “Next” to continue.



The screenshot shows the 'Active Directory Installation Wizard' window. The title bar is blue with the text 'Active Directory Installation Wizard' and a close button. The main window has a white header area with the title 'Domain Controller Type' and a subtitle 'Specify the role you want this server to have.' To the right of the header is a blue icon of a server. The main content area is light gray and contains the question 'Do you want this server to become a domain controller for a new domain or an additional domain controller for an existing domain?'. There are two radio buttons: 'Domain controller for a new domain' (which is selected) and 'Additional domain controller for an existing domain'. Below the first option is a warning icon (yellow triangle with an exclamation mark) and text stating that proceeding will delete all local accounts, cryptographic keys, and encrypted data. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.


Active Directory Installation Wizard

Domain Controller Type
Specify the role you want this server to have.

Do you want this server to become a domain controller for a new domain or an additional domain controller for an existing domain?

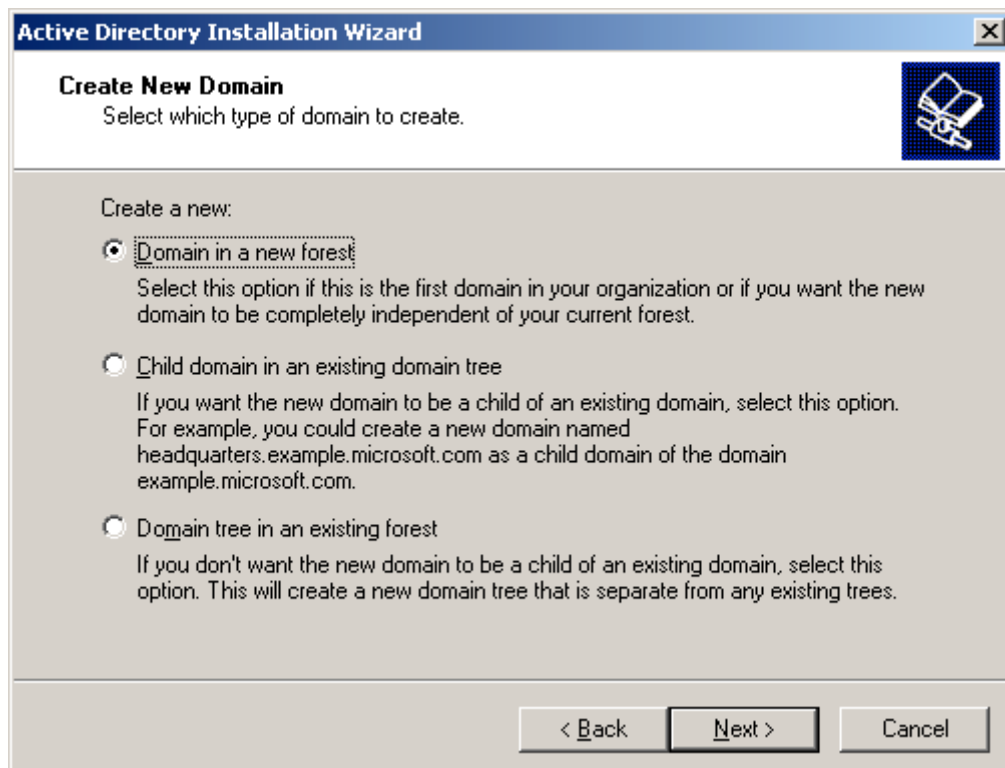
☒ **Domain controller for a new domain**
Select this option to create a new child domain, new domain tree, or new forest. This server will become the first domain controller in the new domain.

☐ **Additional domain controller for an existing domain**

 Proceeding with this option will delete all local accounts on this server.
All cryptographic keys will be deleted and should be exported before continuing.
All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.

< Back Next > Cancel

Next select the “Domain in new forest” radio button, and select “Next” to continue.



The screenshot shows the 'Active Directory Installation Wizard' window. The title bar is blue with the text 'Active Directory Installation Wizard' and a close button. The main window has a white header area with the title 'Create New Domain' and a subtitle 'Select which type of domain to create.' To the right of the header is a blue icon of a server. The main content area is light gray and contains the question 'Create a new:'. There are three radio buttons: 'Domain in a new forest' (which is selected), 'Child domain in an existing domain tree', and 'Domain tree in an existing forest'. Each option has a brief description. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

Active Directory Installation Wizard

Create New Domain
Select which type of domain to create.

Create a new:

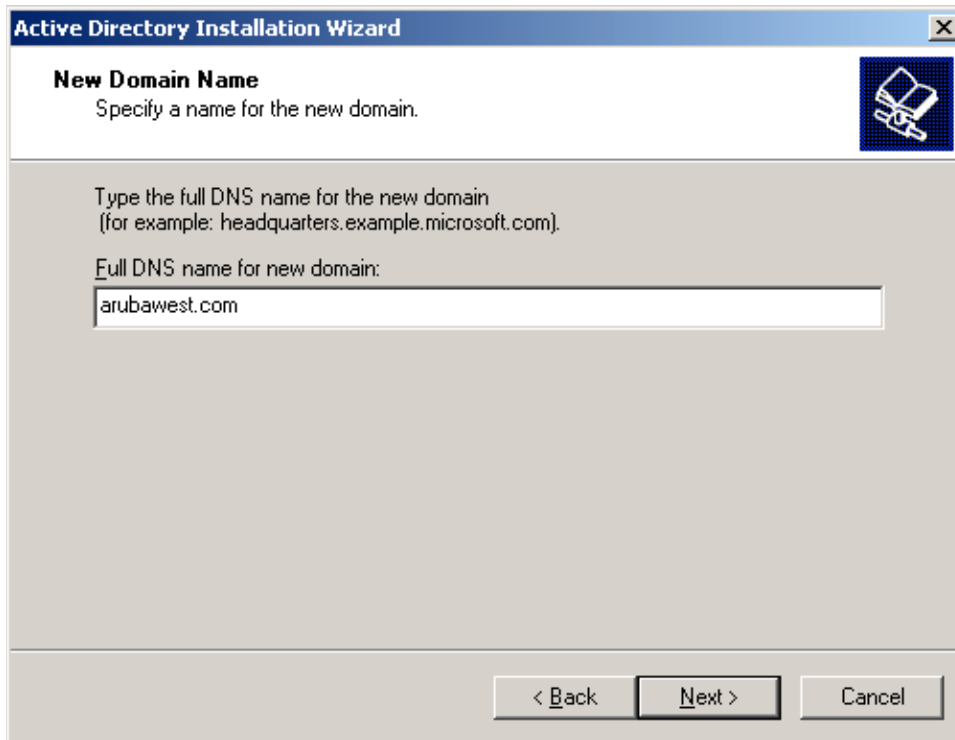
☒ **Domain in a new forest**
Select this option if this is the first domain in your organization or if you want the new domain to be completely independent of your current forest.

☐ **Child domain in an existing domain tree**
If you want the new domain to be a child of an existing domain, select this option. For example, you could create a new domain named headquarters.example.microsoft.com as a child domain of the domain example.microsoft.com.

☐ **Domain tree in an existing forest**
If you don't want the new domain to be a child of an existing domain, select this option. This will create a new domain tree that is separate from any existing trees.

< Back Next > Cancel

At this point you will be asked for the DNS name of the new domain to be created. Enter the desired domain name and select “Next” to continue.



The screenshot shows the 'Active Directory Installation Wizard' window. The title bar is blue with the text 'Active Directory Installation Wizard' and a close button. The main window has a light gray background. At the top, there is a section titled 'New Domain Name' with a subtitle 'Specify a name for the new domain.' and a blue icon of a book with a magnifying glass. Below this, the text reads: 'Type the full DNS name for the new domain (for example: headquarters.example.microsoft.com).' followed by 'Full DNS name for new domain:'. A text input field contains 'arubawest.com'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Active Directory Installation Wizard

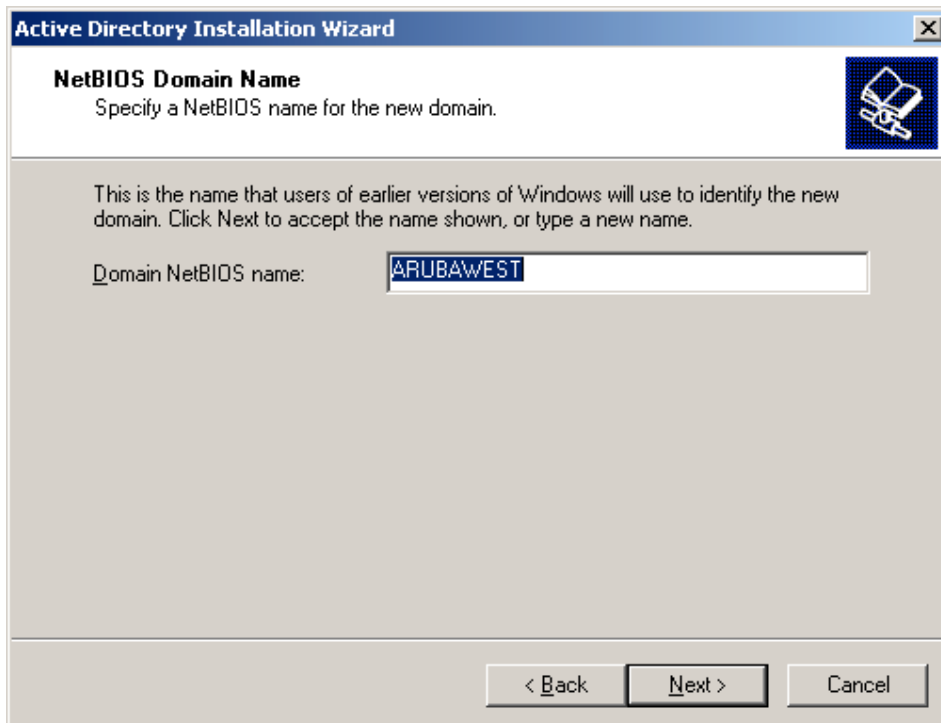
New Domain Name
Specify a name for the new domain.

Type the full DNS name for the new domain
(for example: headquarters.example.microsoft.com).

Full DNS name for new domain:
arubawest.com

< Back Next > Cancel

Next you will be shown the NetBIOS name that will be used for this domain. Select “Next” to continue.



The screenshot shows the 'Active Directory Installation Wizard' window. The title bar is blue with the text 'Active Directory Installation Wizard' and a close button. The main window has a light gray background. At the top, there is a section titled 'NetBIOS Domain Name' with a subtitle 'Specify a NetBIOS name for the new domain.' and a blue icon of a book with a magnifying glass. Below this, the text reads: 'This is the name that users of earlier versions of Windows will use to identify the new domain. Click Next to accept the name shown, or type a new name.' followed by 'Domain NetBIOS name:'. A text input field contains 'ARUBAWEST'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Active Directory Installation Wizard

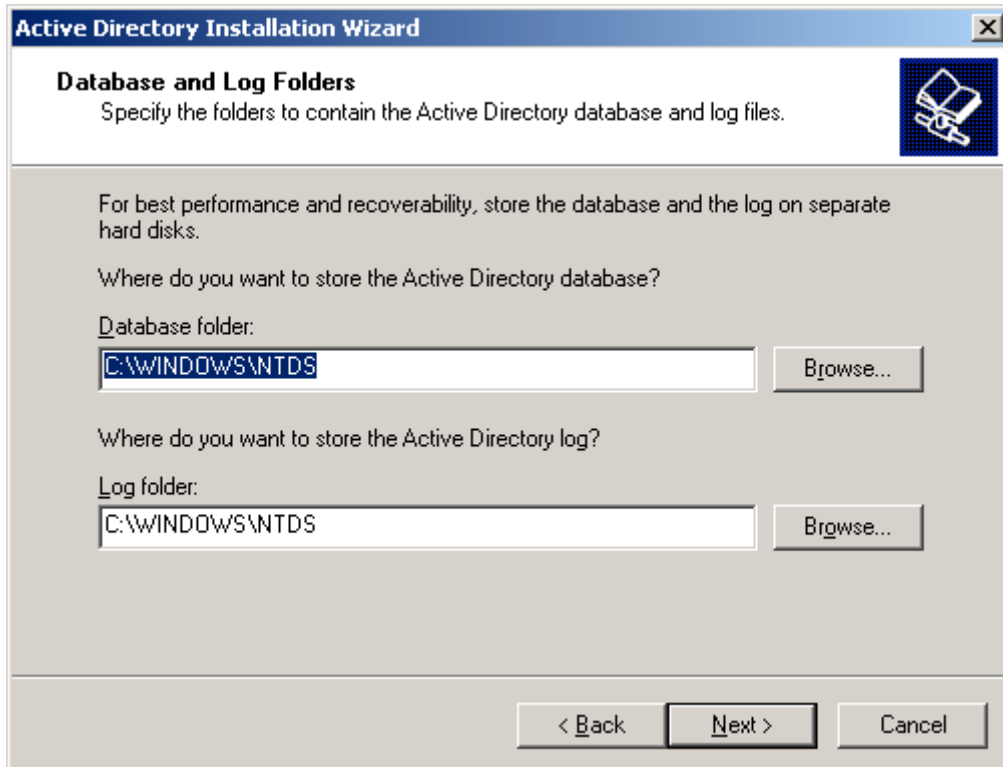
NetBIOS Domain Name
Specify a NetBIOS name for the new domain.

This is the name that users of earlier versions of Windows will use to identify the new domain. Click Next to accept the name shown, or type a new name.

Domain NetBIOS name: ARUBAWEST

< Back Next > Cancel

Now you will be given the option to change the location of the Active Directory database and directory. Just keep the defaults and select “Next” to continue.



The screenshot shows the 'Active Directory Installation Wizard' window, specifically the 'Database and Log Folders' step. The title bar reads 'Active Directory Installation Wizard'. The main heading is 'Database and Log Folders' with a sub-instruction: 'Specify the folders to contain the Active Directory database and log files.' Below this, a note states: 'For best performance and recoverability, store the database and the log on separate hard disks.' The question 'Where do you want to store the Active Directory database?' is followed by a text box labeled 'Database folder:' containing 'C:\WINDOWS\NTDS' and a 'Browse...' button. The next question is 'Where do you want to store the Active Directory log?' followed by a text box labeled 'Log folder:' also containing 'C:\WINDOWS\NTDS' and a 'Browse...' button. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

Active Directory Installation Wizard

Database and Log Folders
Specify the folders to contain the Active Directory database and log files.

For best performance and recoverability, store the database and the log on separate hard disks.

Where do you want to store the Active Directory database?

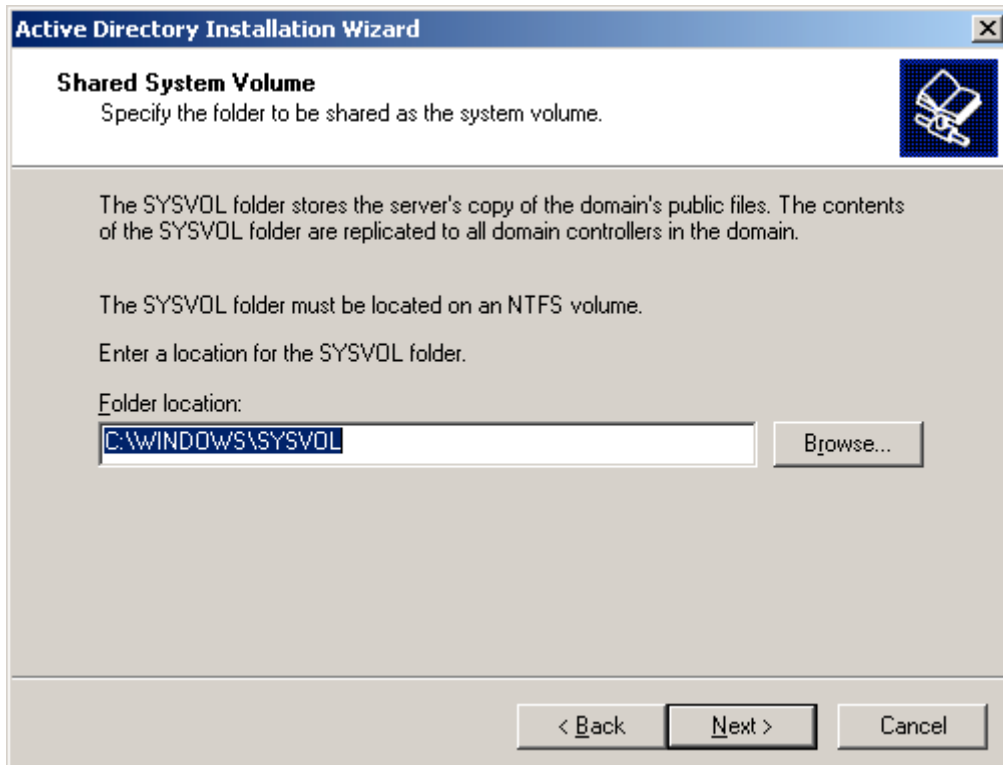
Database folder:
C:\WINDOWS\NTDS Browse...

Where do you want to store the Active Directory log?

Log folder:
C:\WINDOWS\NTDS Browse...

< Back Next > Cancel

Now you can change the location of the Shared System Volume. Select “Next” to continue.



The screenshot shows the 'Active Directory Installation Wizard' window, specifically the 'Shared System Volume' step. The title bar reads 'Active Directory Installation Wizard'. The main heading is 'Shared System Volume' with a sub-instruction: 'Specify the folder to be shared as the system volume.' Below this, a note states: 'The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.' Another note states: 'The SYSVOL folder must be located on an NTFS volume.' The instruction 'Enter a location for the SYSVOL folder.' is followed by a text box labeled 'Folder location:' containing 'C:\WINDOWS\SYSVOL' and a 'Browse...' button. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

Active Directory Installation Wizard

Shared System Volume
Specify the folder to be shared as the system volume.

The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.

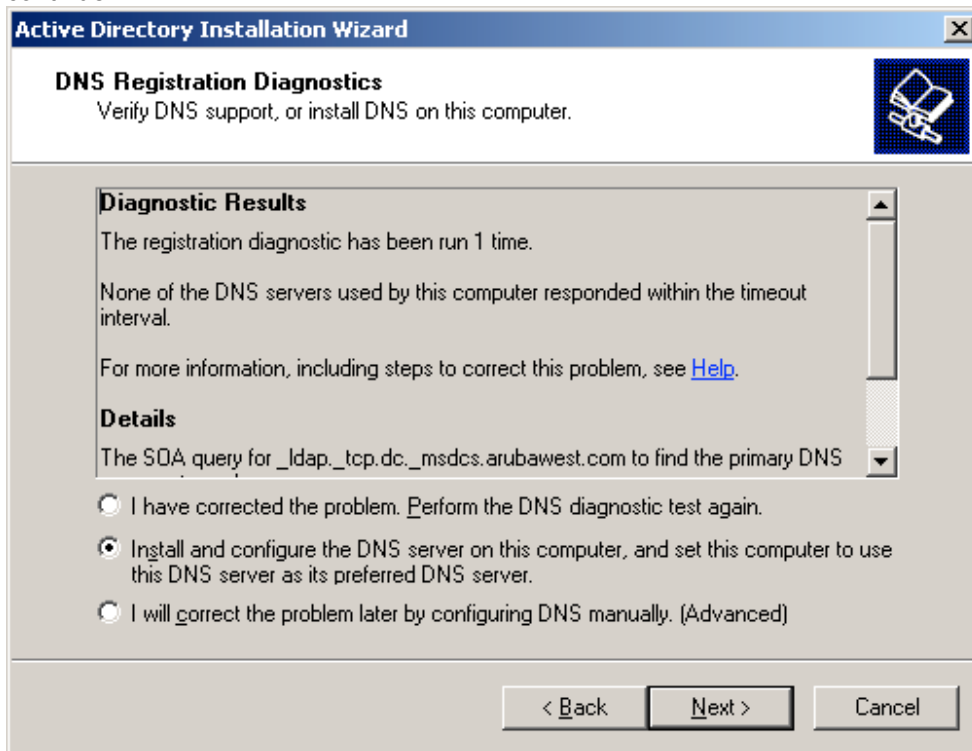
The SYSVOL folder must be located on an NTFS volume.

Enter a location for the SYSVOL folder.

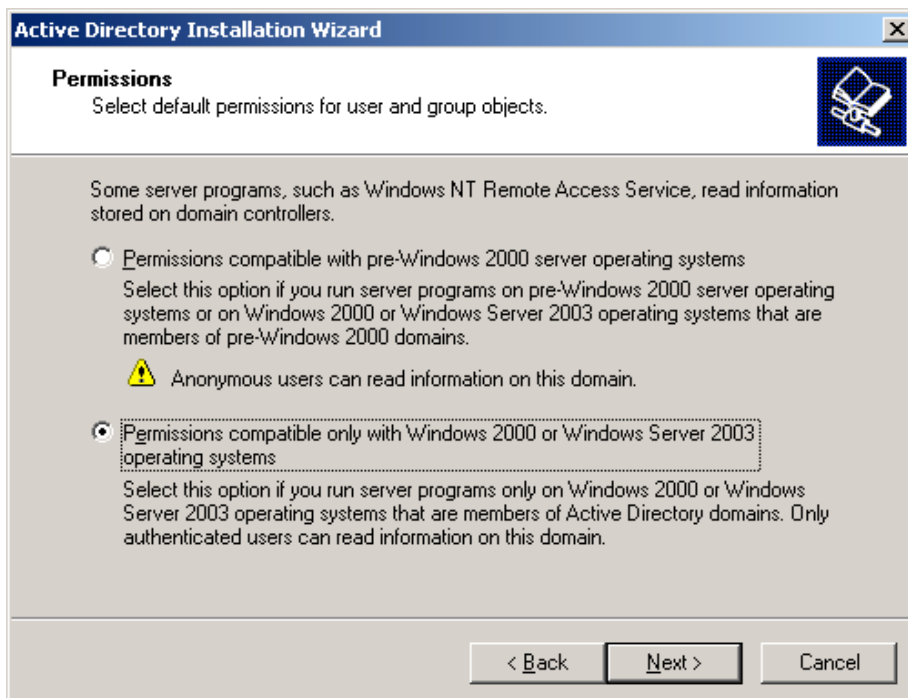
Folder location:
C:\WINDOWS\SYSVOL Browse...

< Back Next > Cancel

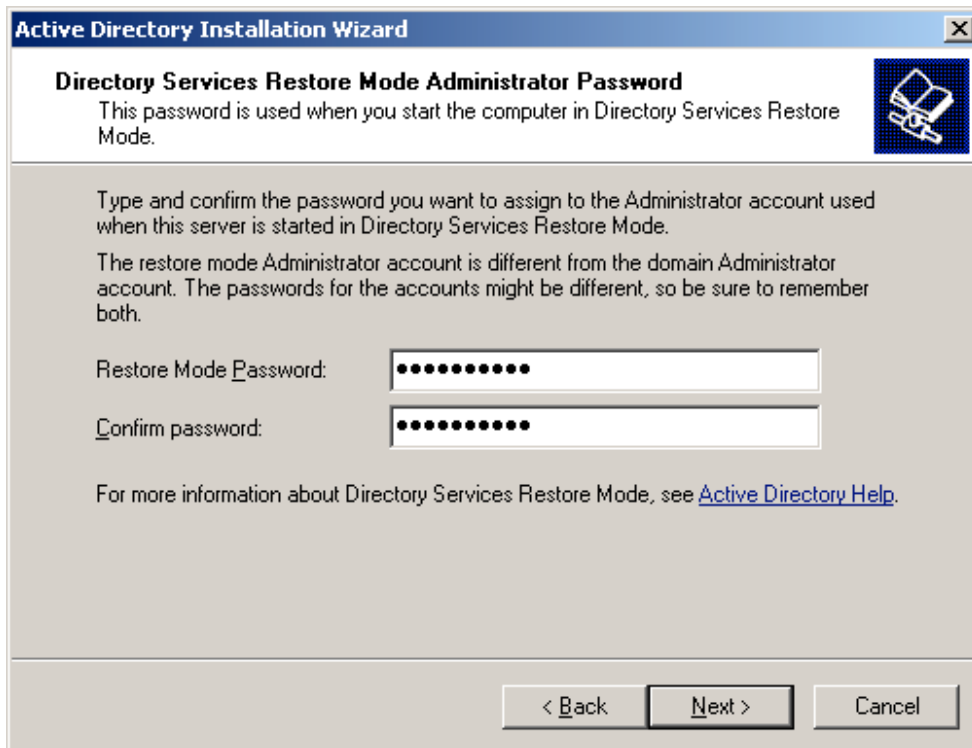
At this point the wizard will give you the option of installing DNS on this server. If you ever want to add a computer to this domain, it will be necessary for that computer to have access to the DNS for this domain. Since this is a fictitious domain, it works best if this server also acts as the DNS server. Select "Install and configure the DNS server" as show below and select "Next" to continue.



You will be asked if you need to support any pre-Windows 2000 operating systems will need to be supported. Select "Next" to continue.



You will now be prompted for a Restore Mode Password. Enter and confirm the password and select "Next" to continue.



Active Directory Installation Wizard

Directory Services Restore Mode Administrator Password
This password is used when you start the computer in Directory Services Restore Mode.

Type and confirm the password you want to assign to the Administrator account used when this server is started in Directory Services Restore Mode.

The restore mode Administrator account is different from the domain Administrator account. The passwords for the accounts might be different, so be sure to remember both.

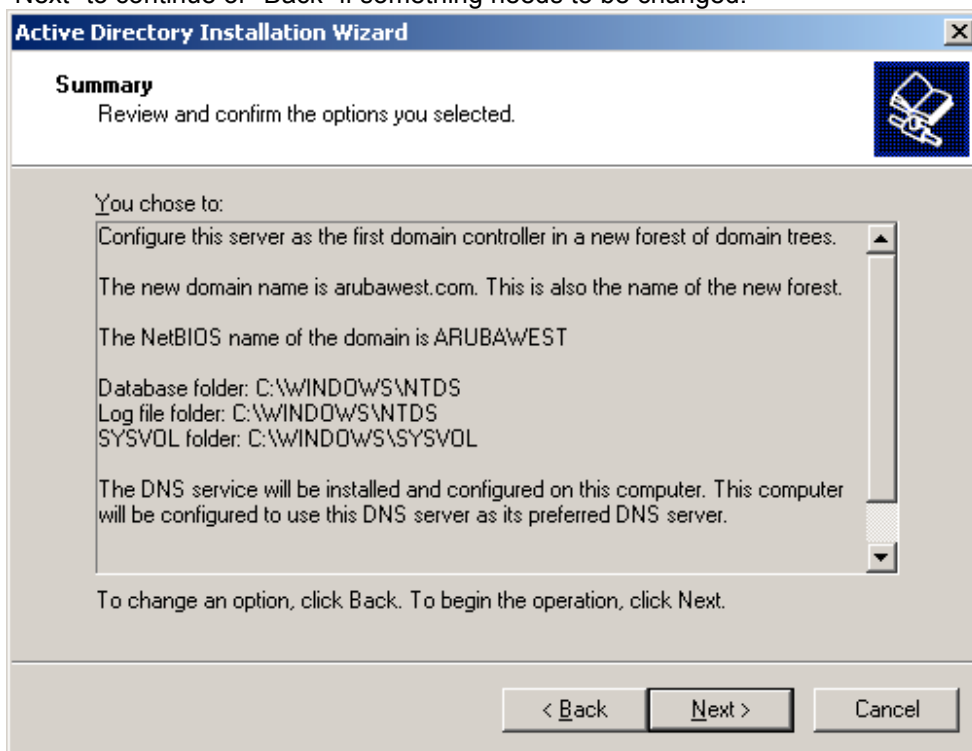
Restore Mode Password:

Confirm password:

For more information about Directory Services Restore Mode, see [Active Directory Help](#).

< Back Next > Cancel

You will now be given an opportunity to review your config options before they are applied. Press "Next" to continue or "Back" if something needs to be changed.



Active Directory Installation Wizard

Summary
Review and confirm the options you selected.

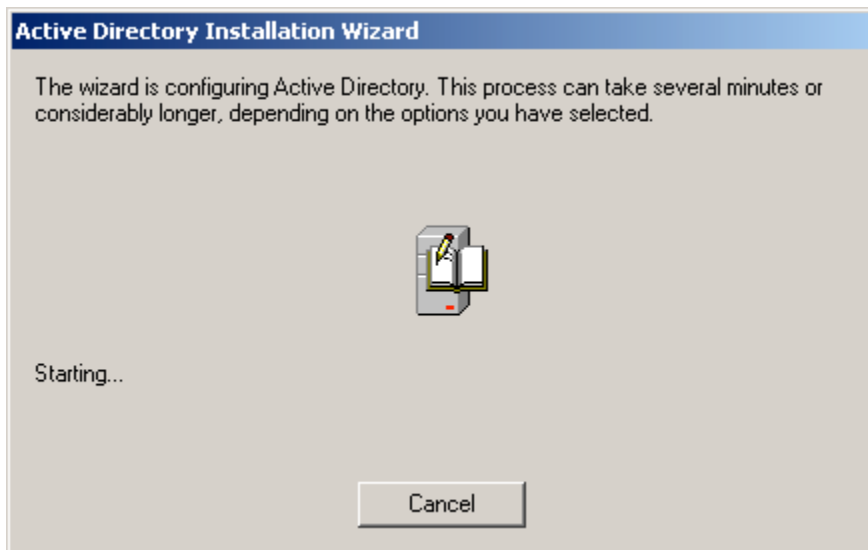
You chose to:

- Configure this server as the first domain controller in a new forest of domain trees.
- The new domain name is arubawest.com. This is also the name of the new forest.
- The NetBIOS name of the domain is ARUBA\WEST
- Database folder: C:\WINDOWS\NTDS
- Log file folder: C:\WINDOWS\NTDS
- SYSVOL folder: C:\WINDOWS\SYSVOL
- The DNS service will be installed and configured on this computer. This computer will be configured to use this DNS server as its preferred DNS server.

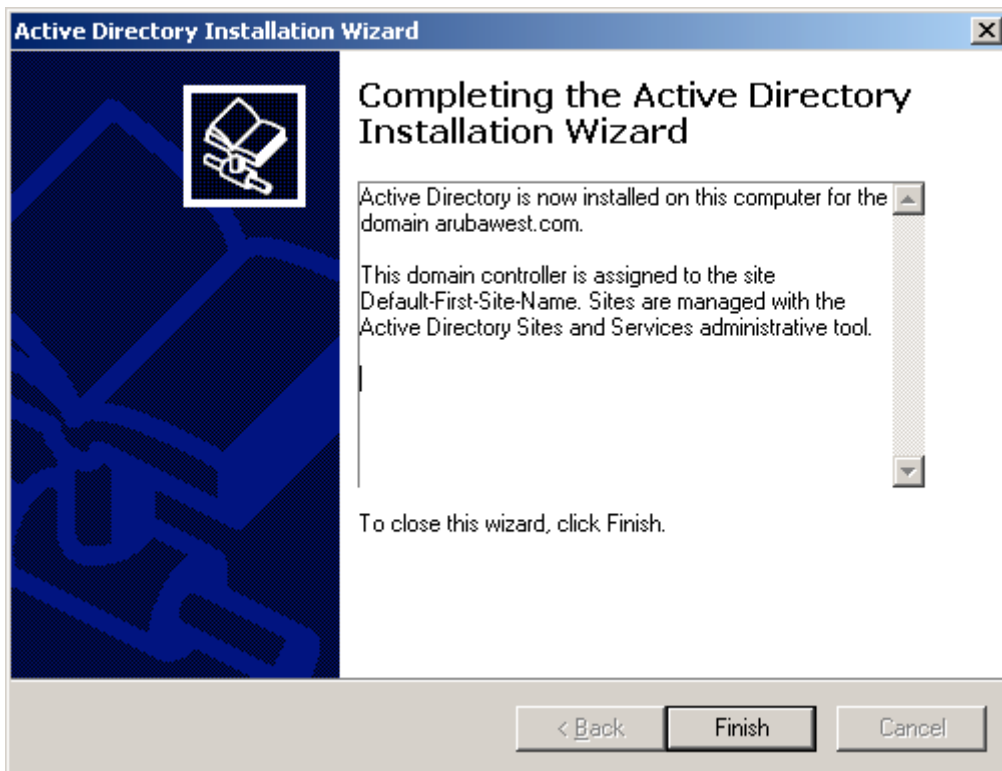
To change an option, click Back. To begin the operation, click Next.

< Back Next > Cancel

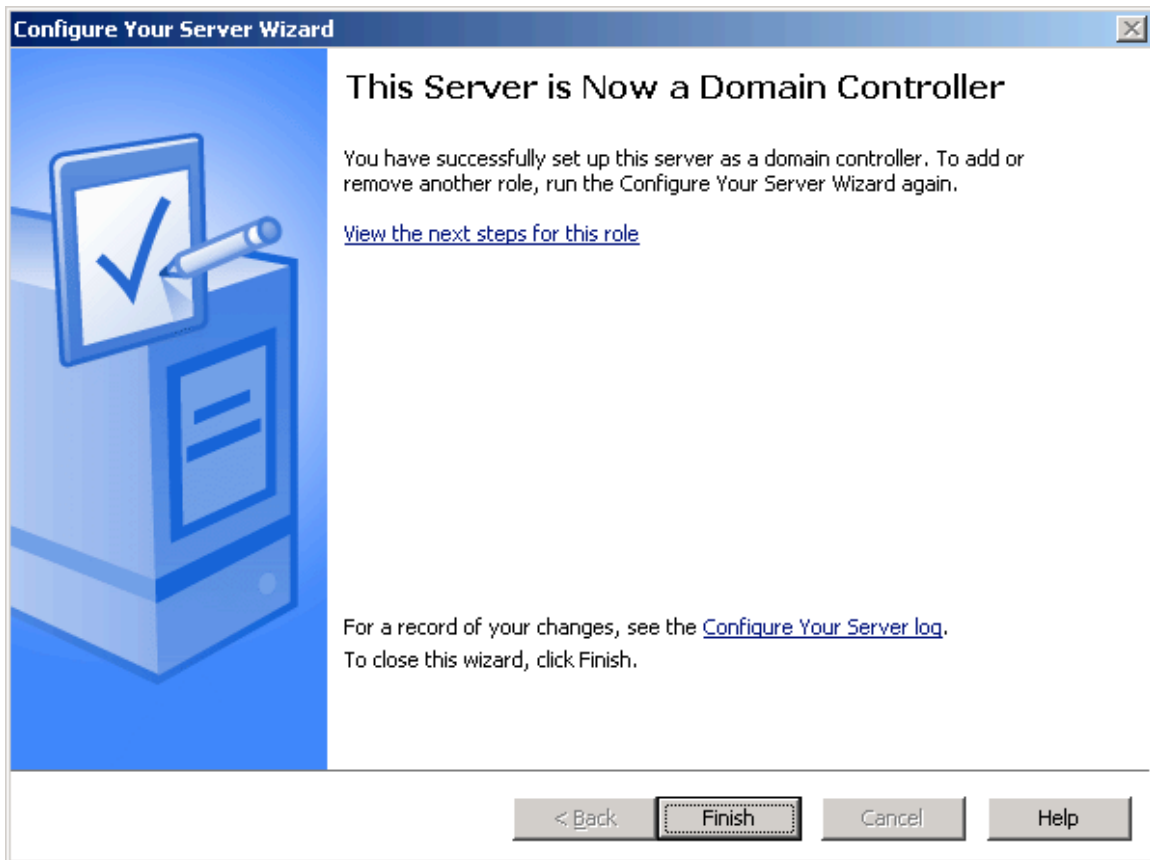
At this point the Active Directory Installation Wizard will install and configure AD based on all of your previous selections. This could take several minutes to complete.



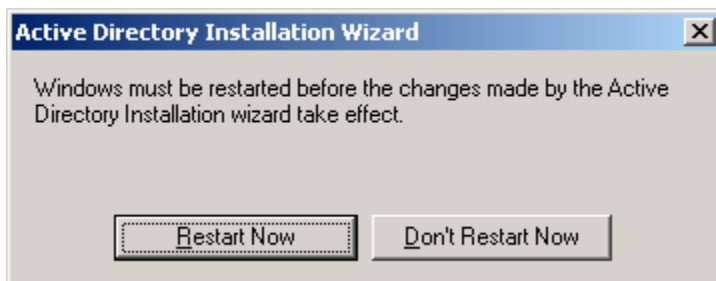
When the Wizard finished the following window will be displayed. Select "Finish" to continue.



You are now finished with the Active Directory configuration, and your server is now a Domain Controller. Select "Finish" to continue.

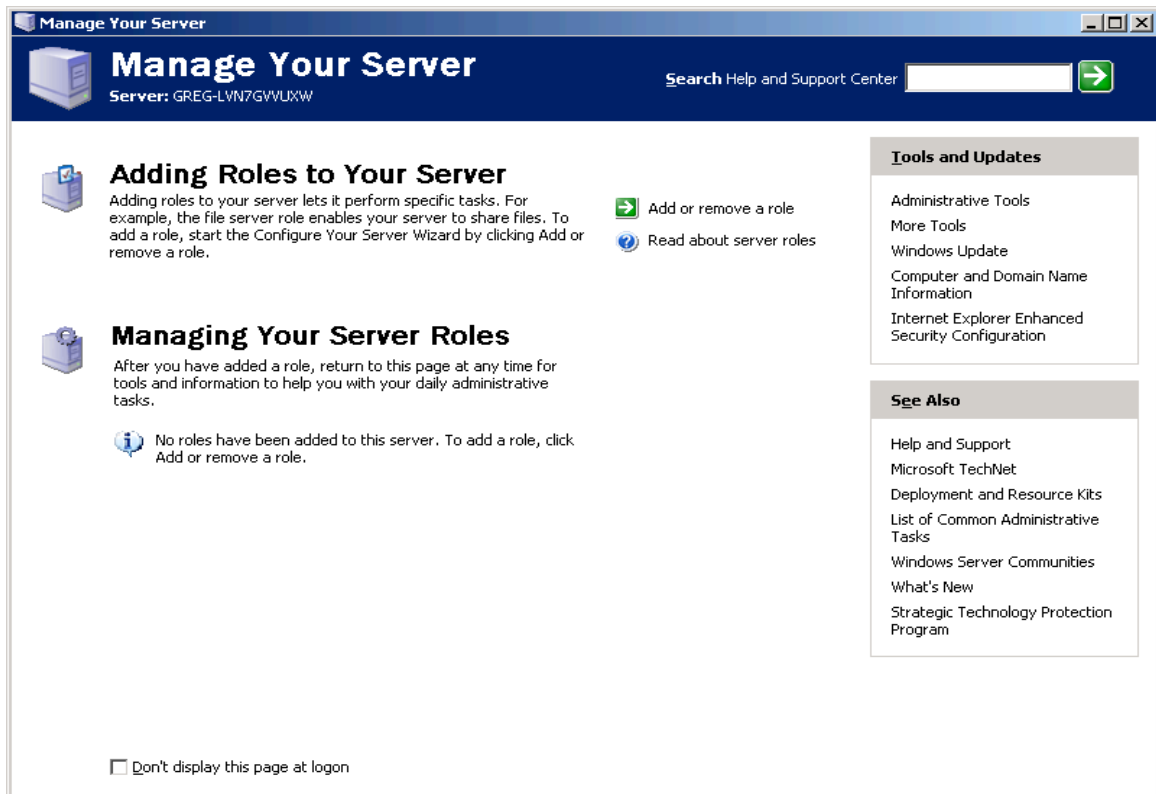


At this point you must restart the system. Select "Restart Now" and the server will reboot.



Enable IIS on the Server

As Discussed before you will need to enable IIS so that Certificate Services are available via the web once we configure the server to be a Certificate Authority. This should be done before Configuring the CA so that all CA components are installed properly. This install will start by adding another role for your server using the window below. Select "Add or remove role" to start adding the IIS features.



Now select “Application server(IIS, ASP.NET)” and select “Next” to continue.

The screenshot shows the 'Configure Your Server Wizard' window at the 'Server Role' step. The title bar reads 'Configure Your Server Wizard'. Below the title bar, the section 'Server Role' is followed by a paragraph: 'You can set up this server to perform one or more specific roles. If you want to add more than one role to this server, you can run this wizard again.' To the right of this text is a small icon of a server with a checkmark. Below the paragraph is a table with two columns: 'Server Role' and 'Configured'. The table lists various server roles and their configuration status. The 'Application server (IIS, ASP.NET)' role is highlighted. To the right of the table, the section 'Application server (IIS, ASP.NET)' is followed by a paragraph describing application servers and a link 'Read about application servers'. Below this is another link 'View the Configure Your Server log.'. At the bottom of the window are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is highlighted.

Server Role	Configured
File server	No
Print server	No
Application server (IIS, ASP.NET)	No
Mail server (POP3, SMTP)	No
Terminal server	No
Remote access / VPN server	No
Domain Controller (Active Directory)	Yes
DNS server	Yes
DHCP server	No
Streaming media server	No
WINS server	No

Application server (IIS, ASP.NET)

Application servers provide the core technologies required to build, deploy, and operate XML Web Services, Web applications, and distributed applications. Application server technologies include ASP.NET, COM+ and Internet Information Services (IIS).

[Read about application servers](#)

View the [Configure Your Server log](#).

< Back Next > Cancel Help

You will then be asked if you want to install any other tools on the server. You don't need any of these, so just select “Next” to continue.

The screenshot shows the 'Configure Your Server Wizard' window at the 'Application Server Options' step. The title bar reads 'Configure Your Server Wizard'. Below the title bar, the section 'Application Server Options' is followed by a paragraph: 'IIS, COM+, ASP.NET, and Microsoft .NET Framework are installed automatically for this role.' To the right of this text is a small icon of a server with a checkmark. Below the paragraph is a section 'Select the additional tools that you want to install on this server.' followed by two checkboxes: 'FrontPage Server Extensions' and 'Enable ASP.NET'. Each checkbox has a descriptive paragraph below it. At the bottom of the window are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is highlighted.

Application Server Options

IIS, COM+, ASP.NET, and Microsoft .NET Framework are installed automatically for this role.

Select the additional tools that you want to install on this server.

☐ FrontPage Server Extensions

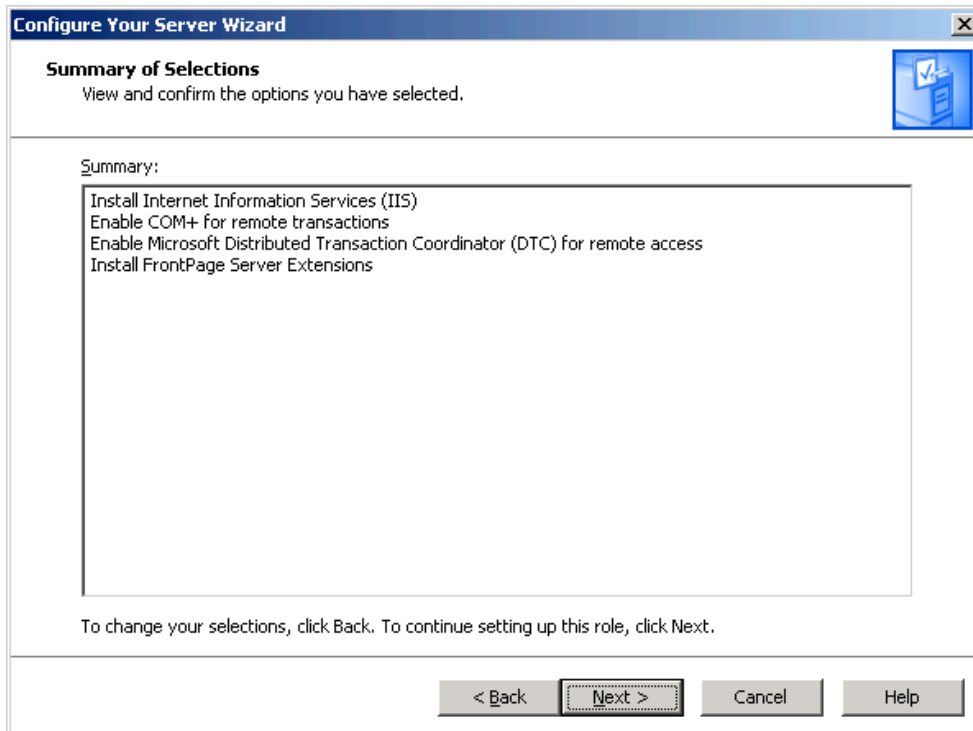
FrontPage Server Extensions are a set of Web server extensions that you can use to publish content with FrontPage, Visual Studio, and Web Folders.

☐ Enable ASP.NET

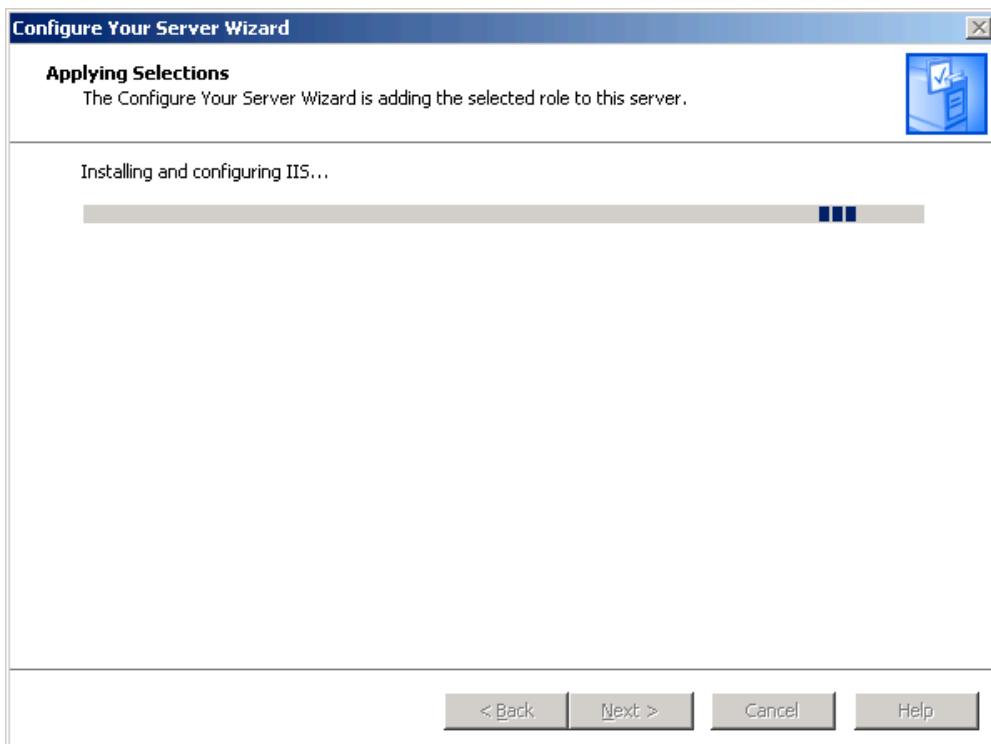
ASP.NET is a powerful programming framework for building Web-based applications and services that can target any browser or device.

< Back Next > Cancel Help

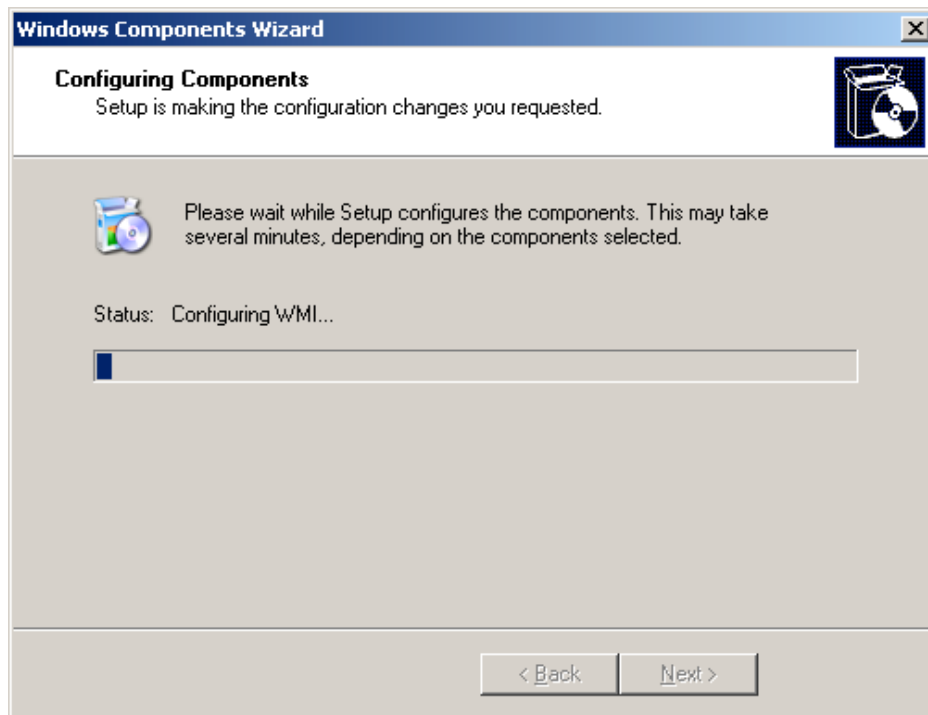
You will now have an opportunity to review your selections. Select “Next” to continue.



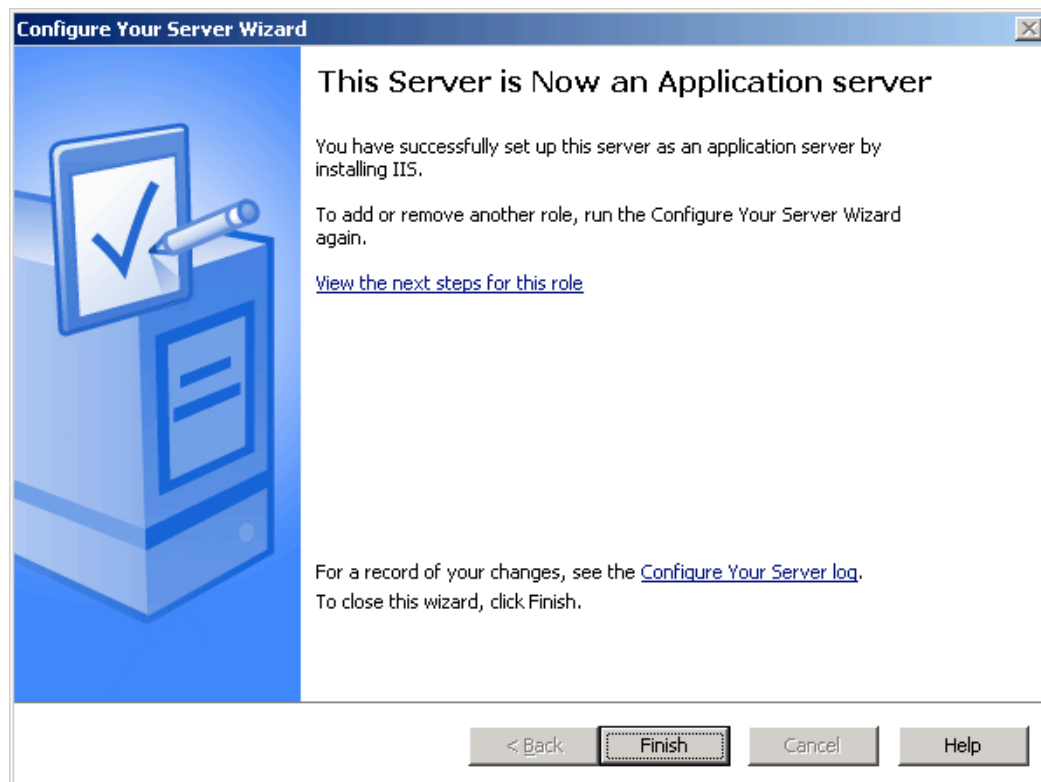
IIS will now be installed.



The wizard will change as IIS continues to be installed.

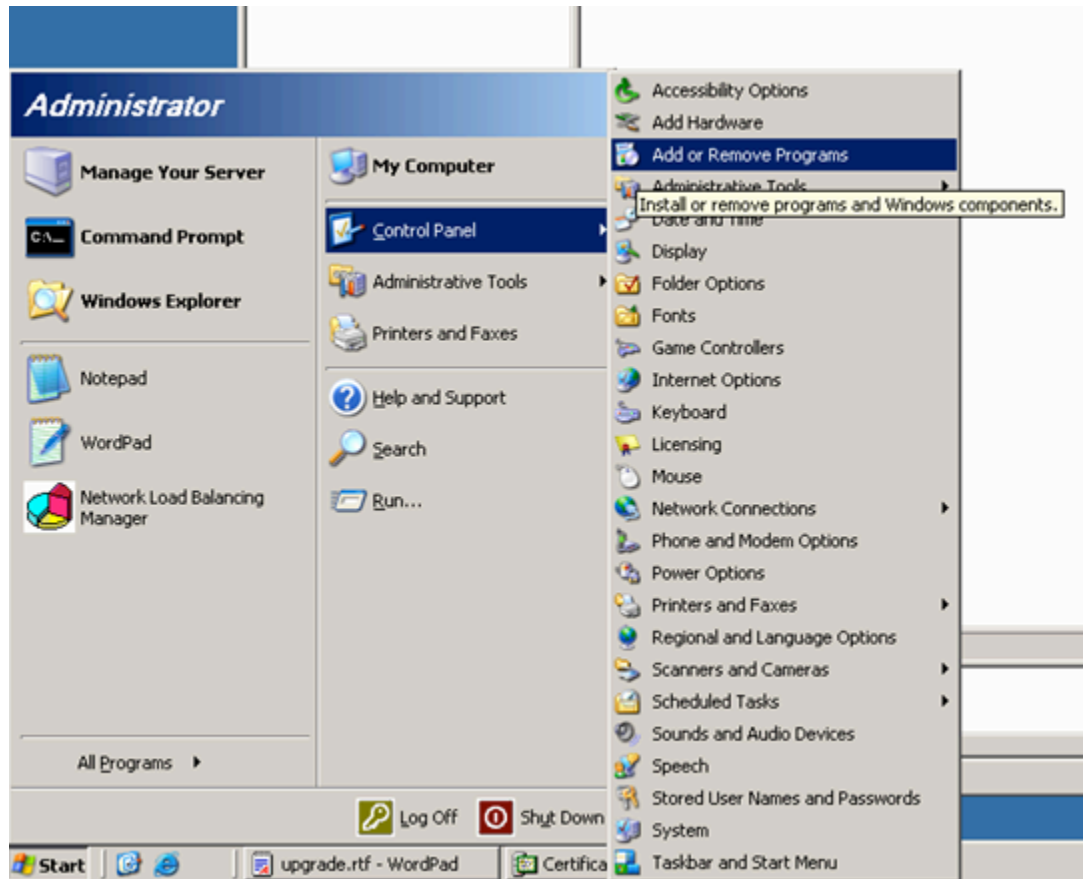


When IIS is finished installing you will see the window below.

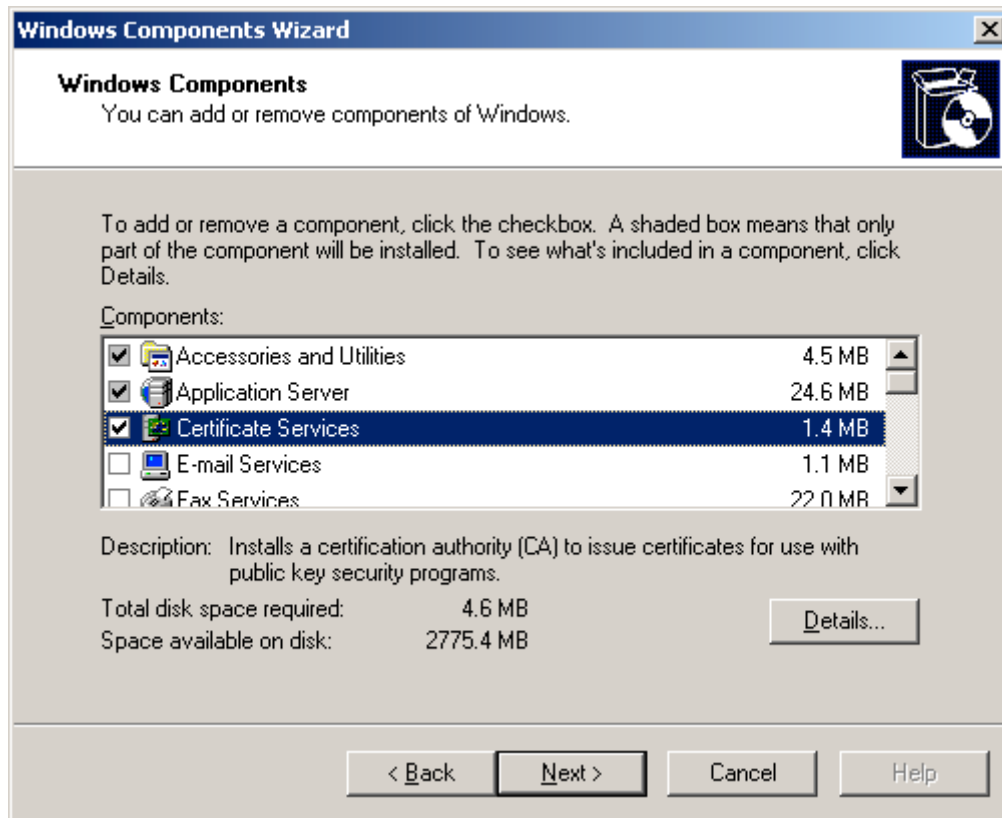


Configure the Server as a Certificate Authority

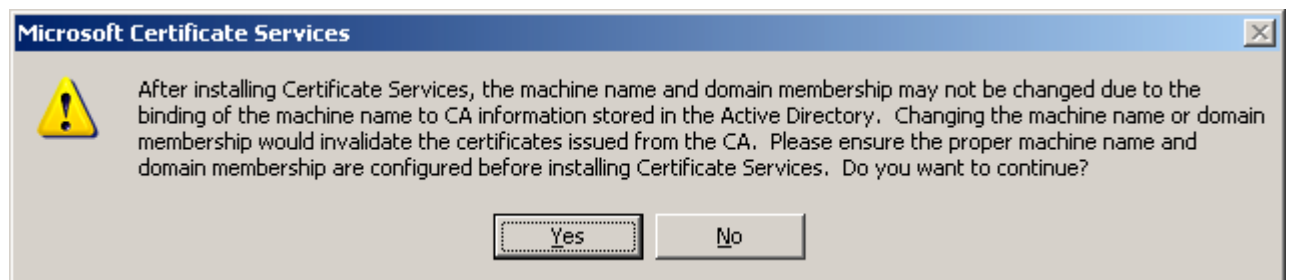
You can now configure the server to be a Certificate Authority. Start the process by selecting Start> Control Panel> Add or Remove Programs as shown below.



Select "Windows Components" and a list of windows components will be displayed. Now check the box next to "Certificate Services" and select "Next".



You will see the following message. Press "Yes" to continue.



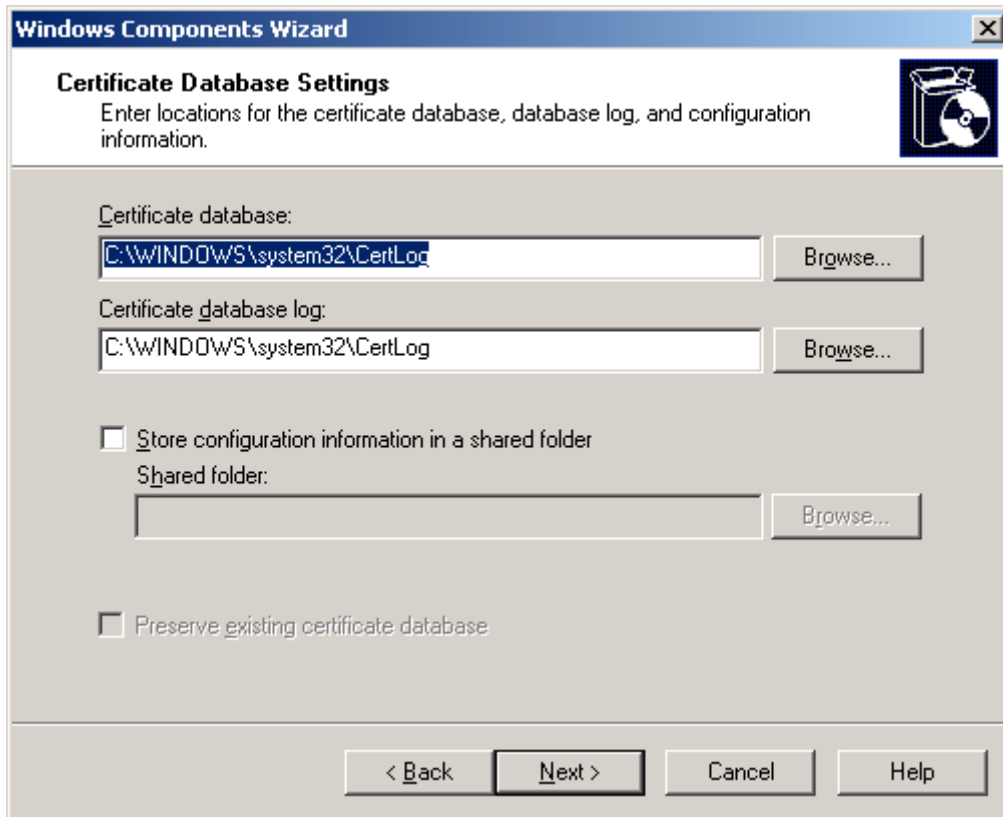
Now select the “Enterprise root CA” radio button, and select “Next” to continue.

The screenshot shows the 'Windows Components Wizard' window with the title 'CA Type'. Below the title bar, it says 'Select the type of CA you want to set up.' There are four radio button options: 'Enterprise root CA' (selected), 'Enterprise subordinate CA', 'Stand-alone root CA', and 'Stand-alone subordinate CA'. Below these is a text box labeled 'Description of CA type' containing the text: 'The most trusted CA in an enterprise. Should be installed before any other CA.' At the bottom, there is a checkbox labeled 'Use custom settings to generate the key pair and CA certificate' which is unchecked. Navigation buttons at the bottom include '< Back', 'Next >', 'Cancel', and 'Help'.

At this point you will ask for the Common Name for the CA. The CN “ArubawestCSVR” was used in the example below. Select “Next” to continue.

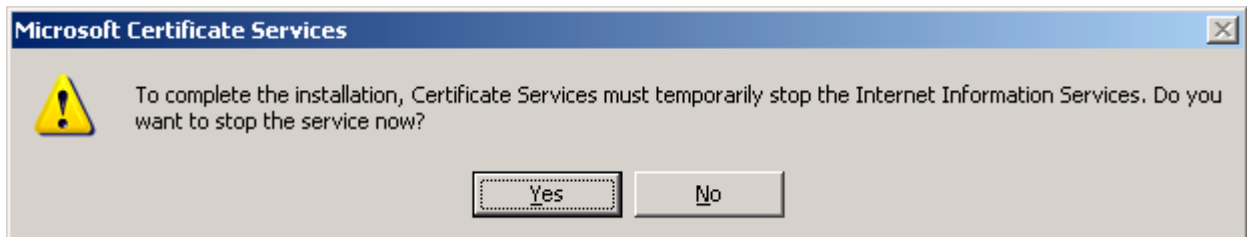
The screenshot shows the 'Windows Components Wizard' window with the title 'CA Identifying Information'. Below the title bar, it says 'Enter information to identify this CA.' There are three text input fields: 'Common name for this CA:' with the value 'ArubawestCSVR', 'Distinguished name suffix:' with the value 'DC=arubawest,DC=com', and 'Preview of distinguished name:' with the value 'CN=ArubawestCSVR,DC=arubawest,DC=com'. At the bottom left, there is a 'Validity period:' section with a text box containing '5' and a dropdown menu set to 'Years'. To the right of this is an 'Expiration date:' section with the value '4/6/2010 10:39 AM'. Navigation buttons at the bottom include '< Back', 'Next >', 'Cancel', and 'Help'.

You will now be given an opportunity to change the location of the database and log files. Just select "Next" to continue.



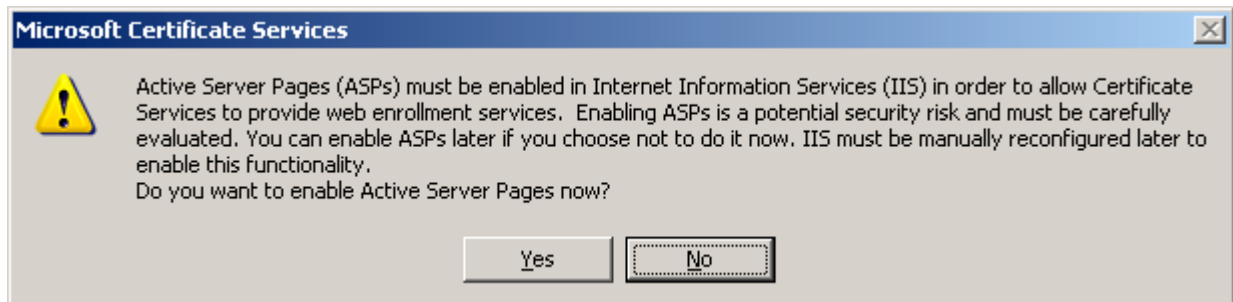
The screenshot shows the "Windows Components Wizard" window with the "Certificate Database Settings" tab selected. The window has a title bar with "Windows Components Wizard" and a close button. Below the title bar is a header area with the tab name and a description: "Enter locations for the certificate database, database log, and configuration information." To the right of the description is a CD-ROM icon. The main area contains three sections: 1. "Certificate database:" with a text box containing "C:\WINDOWS\system32\CertLog" and a "Browse..." button. 2. "Certificate database log:" with a text box containing "C:\WINDOWS\system32\CertLog" and a "Browse..." button. 3. A checkbox labeled "Store configuration information in a shared folder". Below this checkbox is a "Shared folder:" text box and a "Browse..." button. At the bottom of the main area is another checkbox labeled "Preserve existing certificate database". At the very bottom of the window are four buttons: "< Back", "Next >", "Cancel", and "Help".

You will get a warning that IIS will need to be stopped. Select "Yes" to continue.



The screenshot shows a "Microsoft Certificate Services" dialog box with a yellow warning triangle icon. The text inside says: "To complete the installation, Certificate Services must temporarily stop the Internet Information Services. Do you want to stop the service now?". At the bottom are two buttons: "Yes" and "No".

You will get a message stating that Active Server Pages needs to be enabled. Select "Yes" to continue.



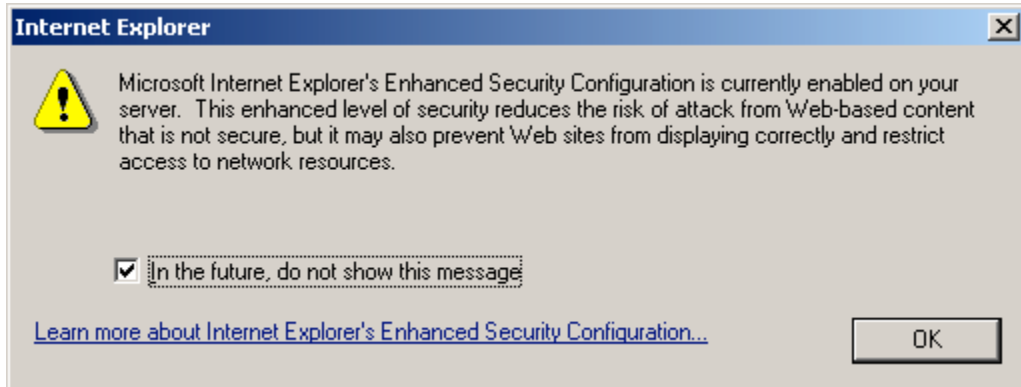
The screenshot shows a "Microsoft Certificate Services" dialog box with a yellow warning triangle icon. The text inside says: "Active Server Pages (ASPs) must be enabled in Internet Information Services (IIS) in order to allow Certificate Services to provide web enrollment services. Enabling ASPs is 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?". At the bottom are two buttons: "Yes" and "No".

At this point the wizard is finished, and the server will now function as a CA.

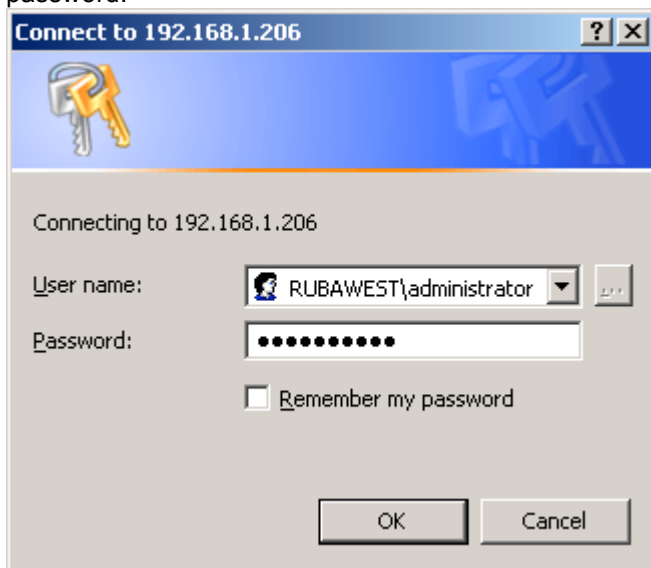


Download the CA Certificate

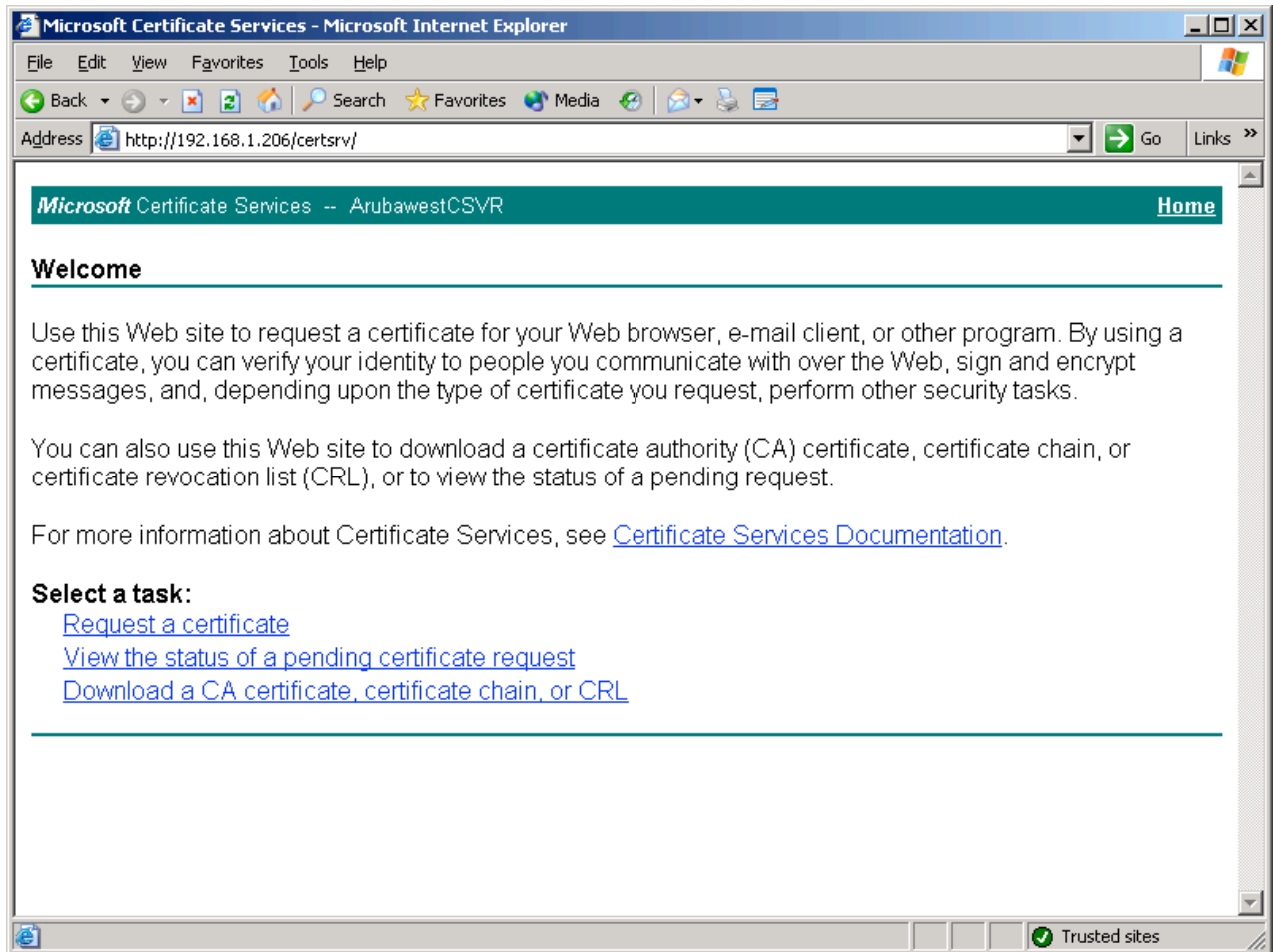
At this point you will need to Download the CA Certificate to make this server a trusted CA on this local machine. To do this you need to open a web browser and browse to the IP of this server and to the /certsrv page. In my case I needed to browse to <http://192.168.1.206/certsrv/>. Internet explorer may show the following warning. Select "OK" to continue.



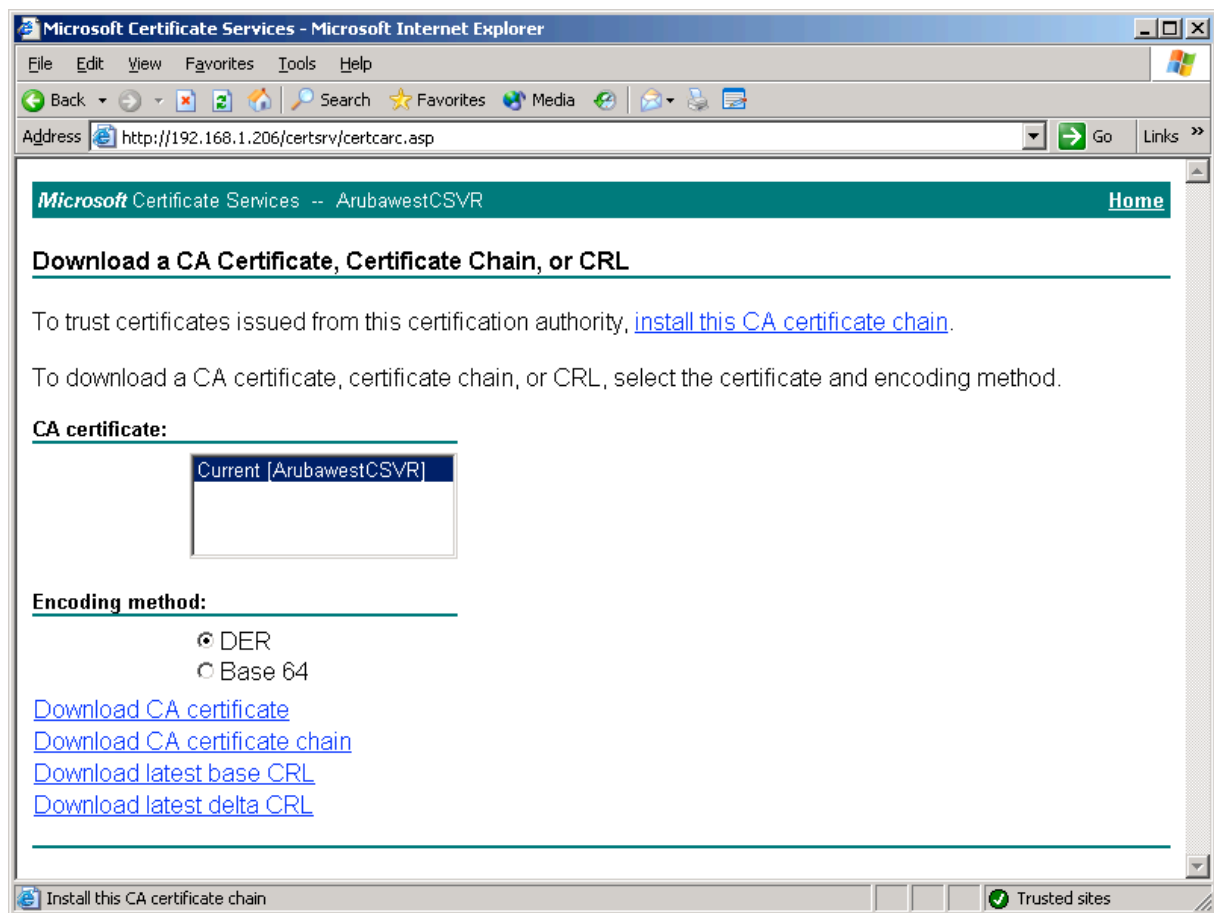
At this point you may be prompted with a login screen. You can use the administrator account and password.



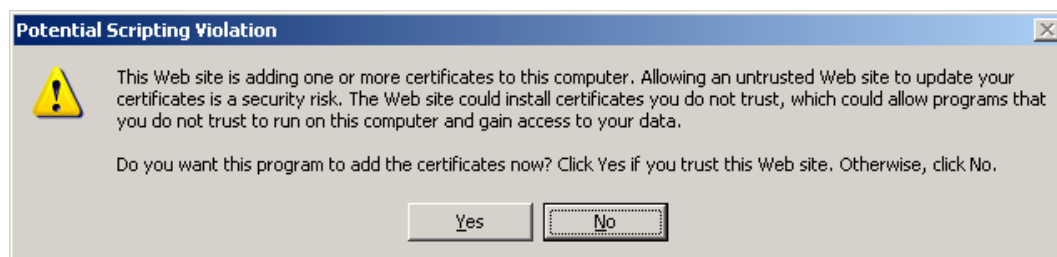
At this point you should see the web page as shown below. Select the link “Download a CA certificate, certificate chain, or CRL.”



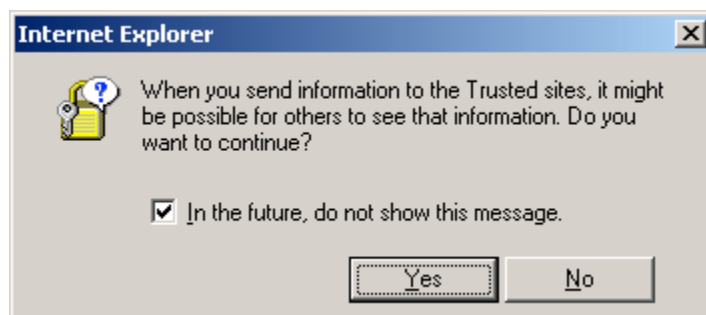
Now you will see the following page. Select the link “Install this CA certificate chain”.

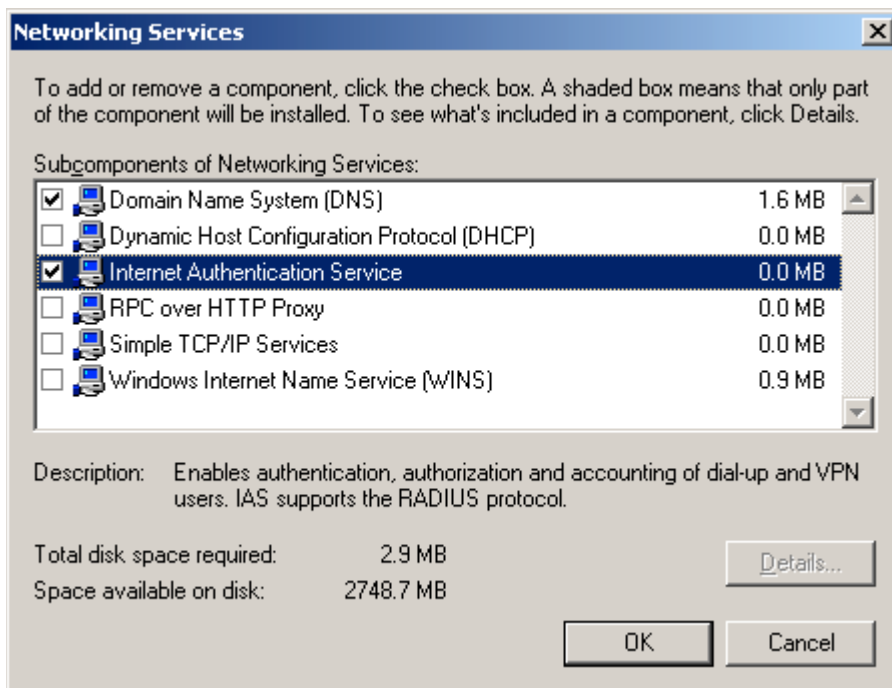
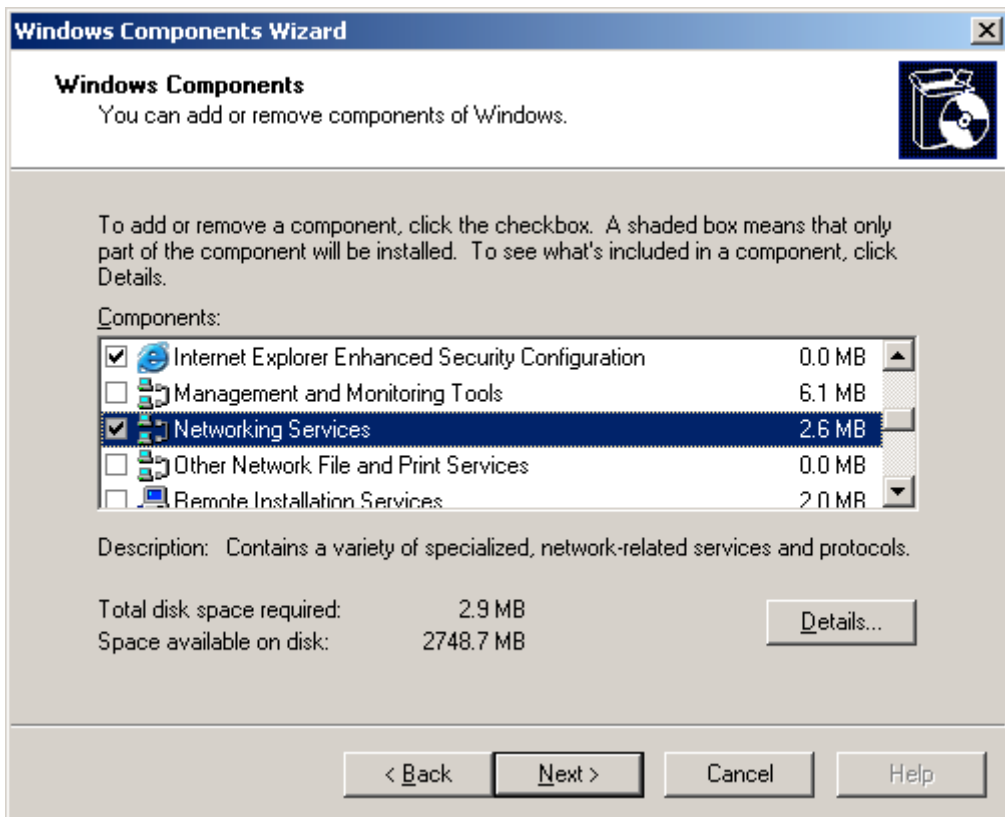


You will be prompted asking if you want to add the certificate. Select “Yes” to continue.



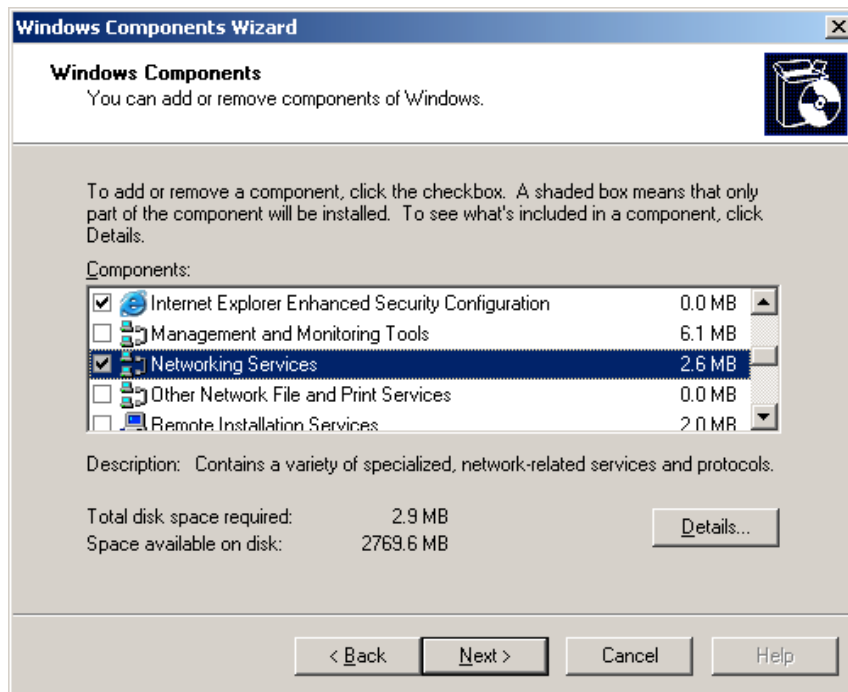
You may also see the following message. Select “Yes” to continue.





Enable and configure IAS

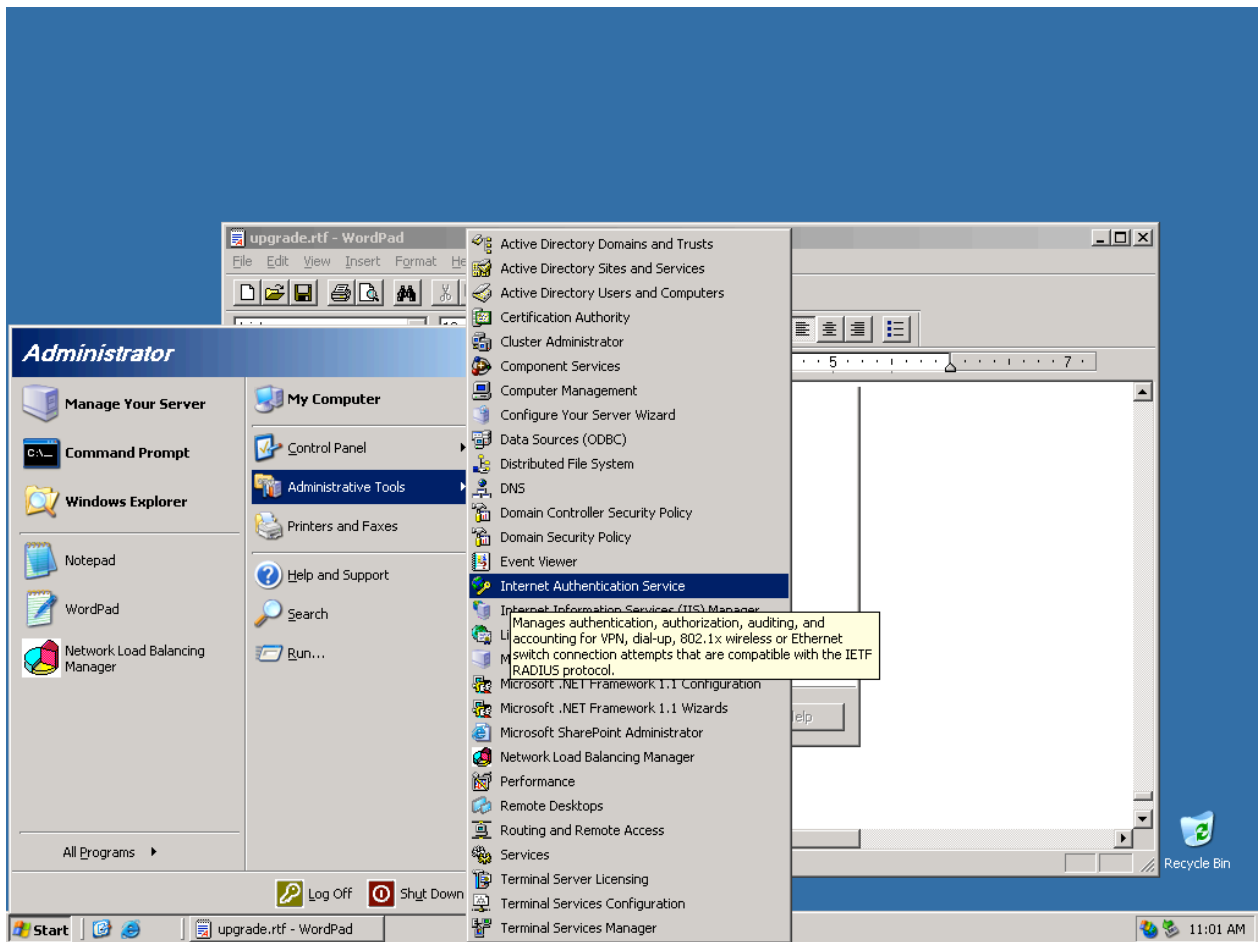
Now we are ready to install and configure IAS. Start the process by bring us the windows component wizard just as we did earlier for installing Certificate Services. Here you need to click on the “Networking Services” line to view all of the available services. Check the box next to “Internet Authentication Service” and select “Next” to continue.



The wizard will complete and you should see the following message.

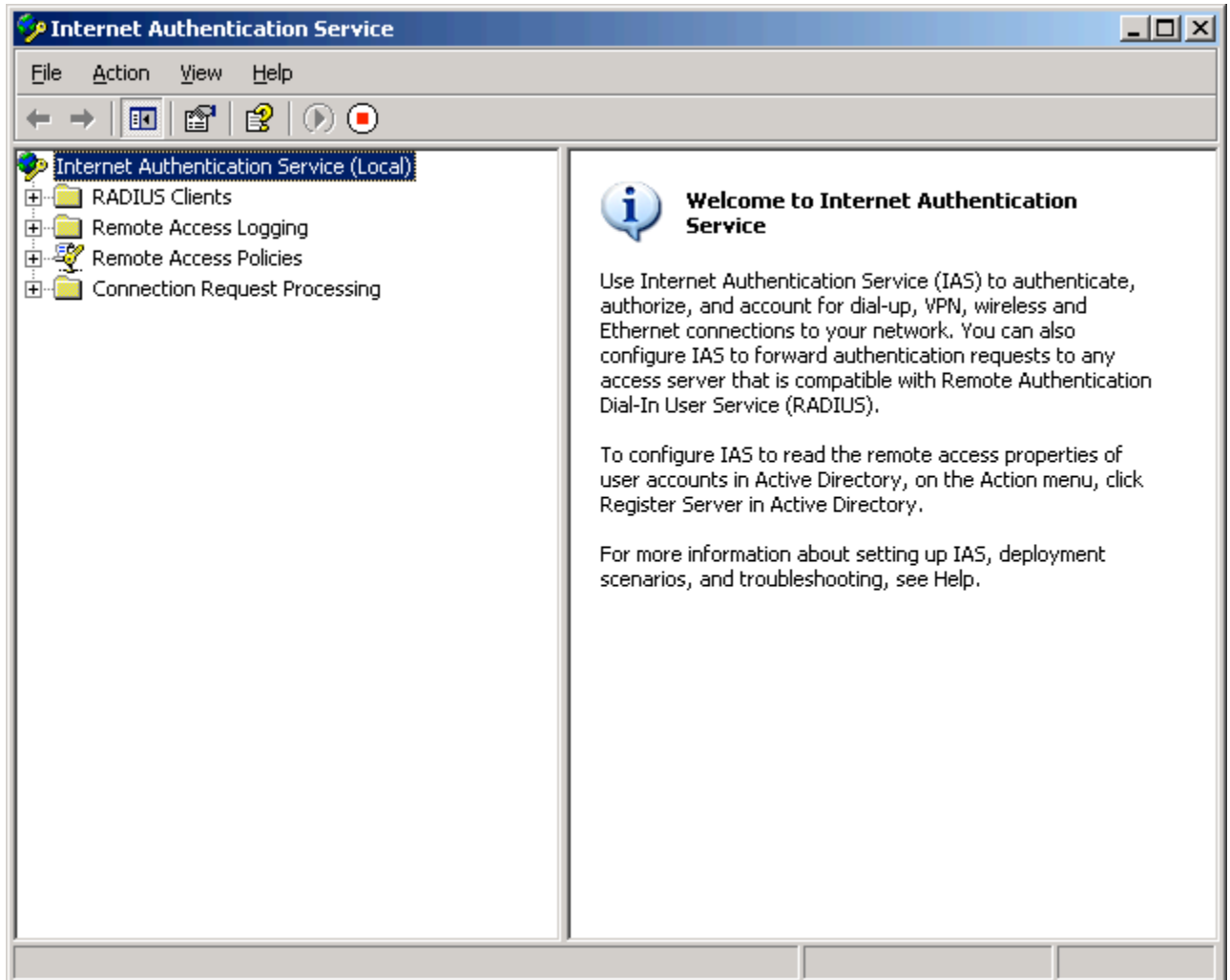


You can now configure IAS by going to Start>Administrative Tools>Internet Authentication Service> .

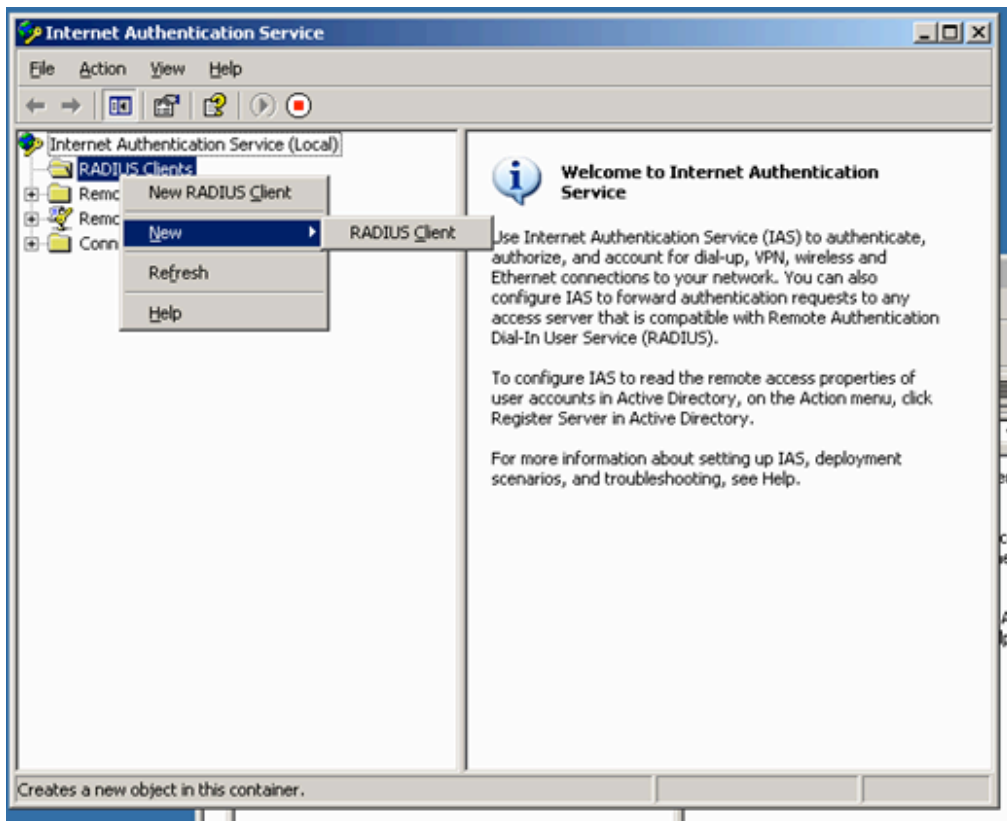


Here you will be presented with the IAS setup GUI.

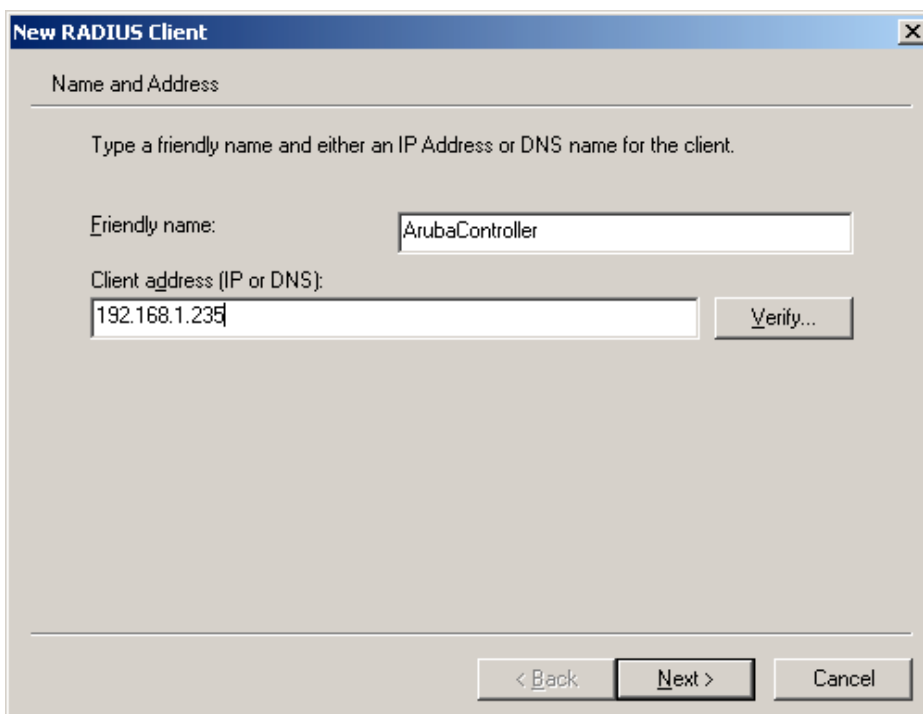
We will need to setup a Radius Client (The Aruba Controller) and a Remote Access Policy to be applied when users are authenticating.



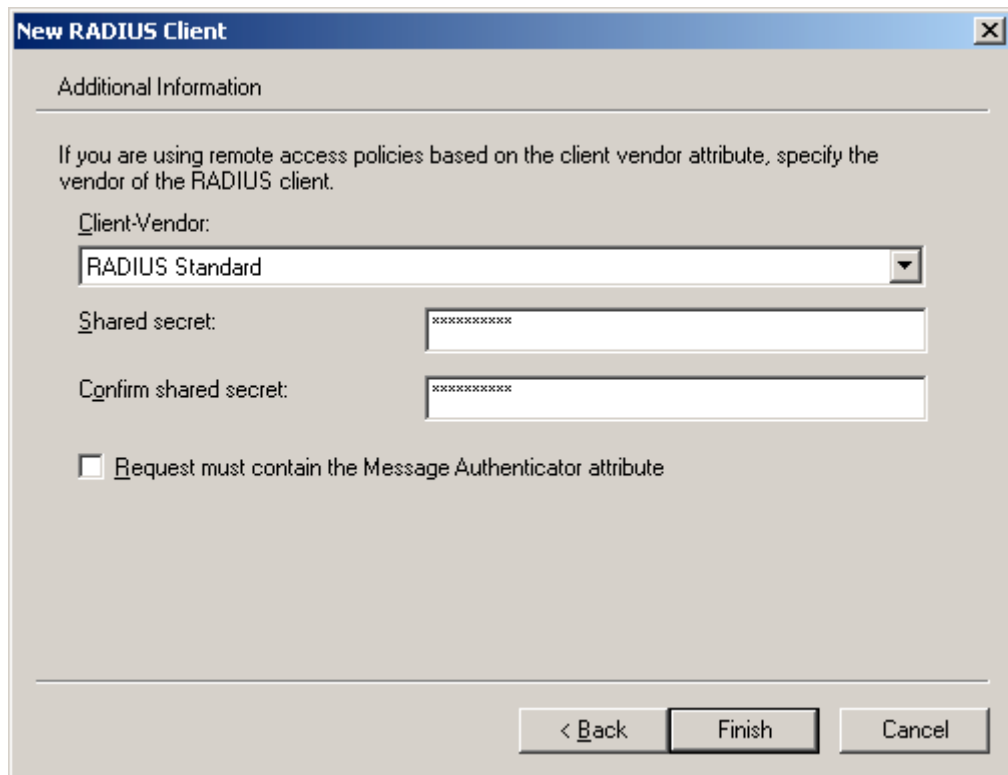
To add a radius client right click on the "Radius Client" folder and select New>Radius client.



You will now see a menu allowing you to assign a Friendly Name, and IP address for the client. Select "Next" to continue.



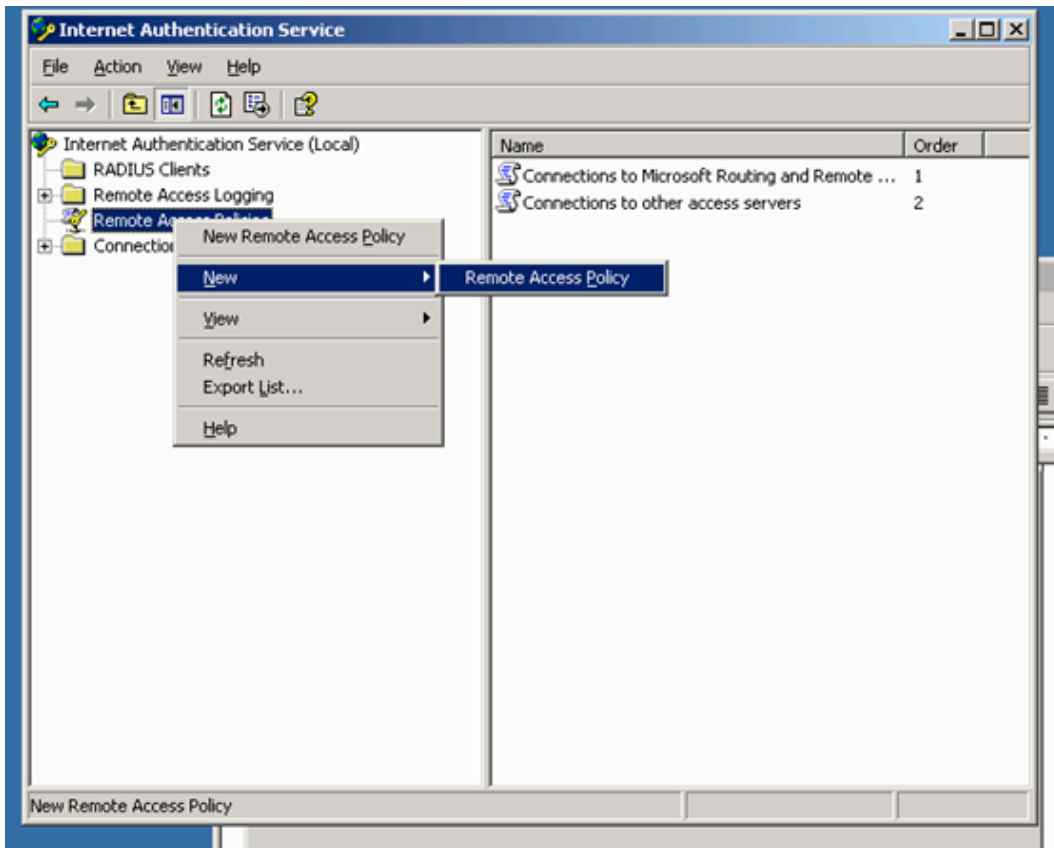
Next you will be asked to select a Client-Vendor, and to define a shared secret. Use RADIUS Standard, and any shared secret you wish. Select "Finish" and the client is now created.



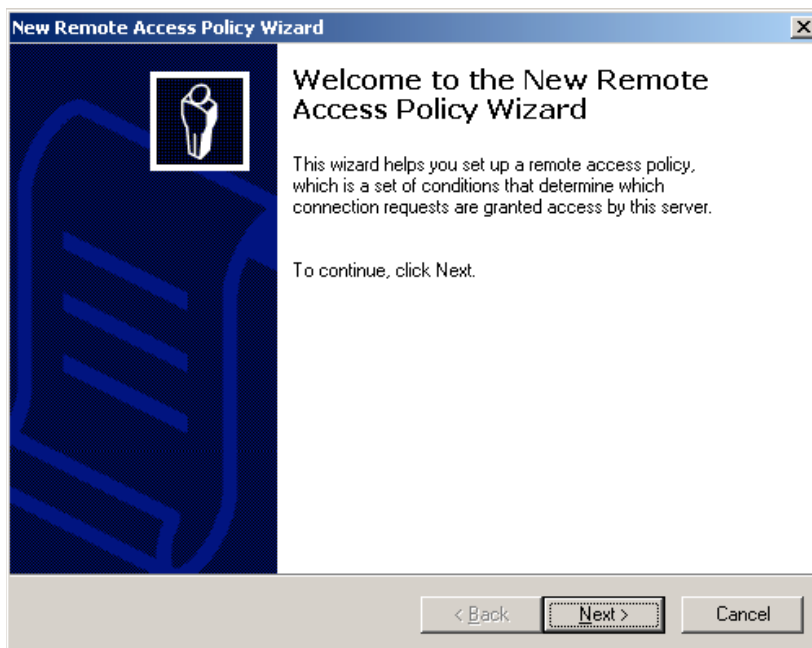
The image shows a Windows-style dialog box titled "New RADIUS Client". It has a blue title bar with a close button (X) in the top right corner. The main area is light gray and contains the following elements:

- A section header "Additional Information" followed by a horizontal line.
- Instructional text: "If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client."
- A label "Client-Vendor:" followed by a dropdown menu currently showing "RADIUS Standard".
- A label "Shared secret:" followed by a text input field containing "xxxxxxxx".
- A label "Confirm shared secret:" followed by a text input field containing "xxxxxxxx".
- A checkbox labeled "Request must contain the Message Authenticator attribute", which is currently unchecked.
- A horizontal line separating the main content from the buttons.
- Three buttons at the bottom: "< Back", "Finish", and "Cancel". The "Finish" button is highlighted with a black border.

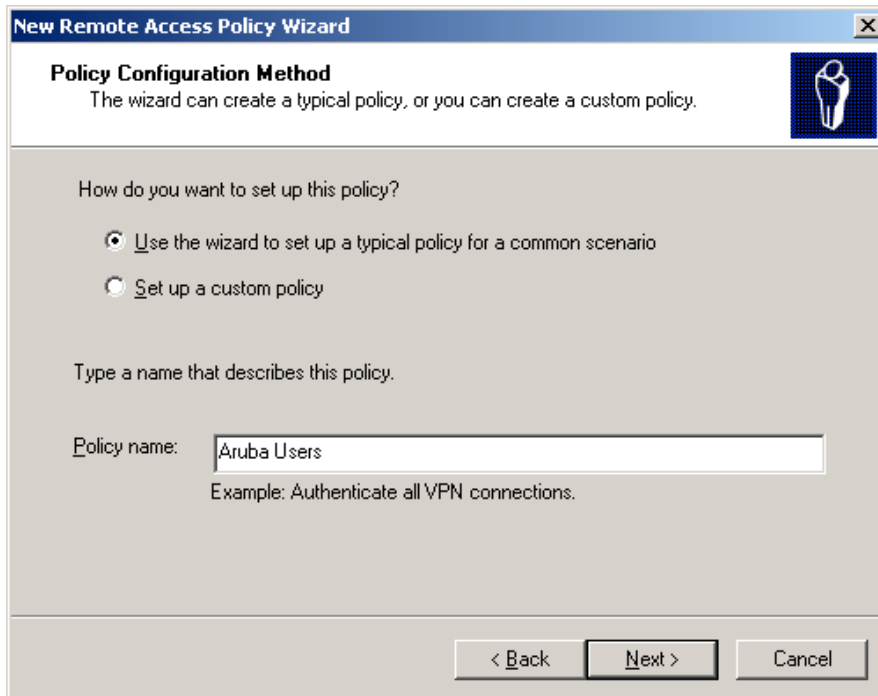
Next we need to create a Remote Access Policy. Again, right click on the Remote Access Policy line, and select New>Remote Access Policy.



Now the Remote Access Policy Wizard will start, Select "Next" to continue.



First you need to give the policy a name, and select “Next” to continue



The screenshot shows the 'New Remote Access Policy Wizard' window, specifically the 'Policy Configuration Method' step. The window has a title bar with the text 'New Remote Access Policy Wizard' and a close button. Below the title bar is a header section with the title 'Policy Configuration Method' and a sub-header 'The wizard can create a typical policy, or you can create a custom policy.' To the right of the header is a small icon of a person. The main area of the window contains the question 'How do you want to set up this policy?' followed by two radio button options: 'Use the wizard to set up a typical policy for a common scenario' (which is selected) and 'Set up a custom policy'. Below these options is a text prompt 'Type a name that describes this policy.' followed by a text input field containing 'Aruba Users'. Below the input field is an example text 'Example: Authenticate all VPN connections.' At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

New Remote Access Policy Wizard

Policy Configuration Method
The wizard can create a typical policy, or you can create a custom policy.

How do you want to set up this policy?

☒ Use the wizard to set up a typical policy for a common scenario

☐ Set up a custom policy

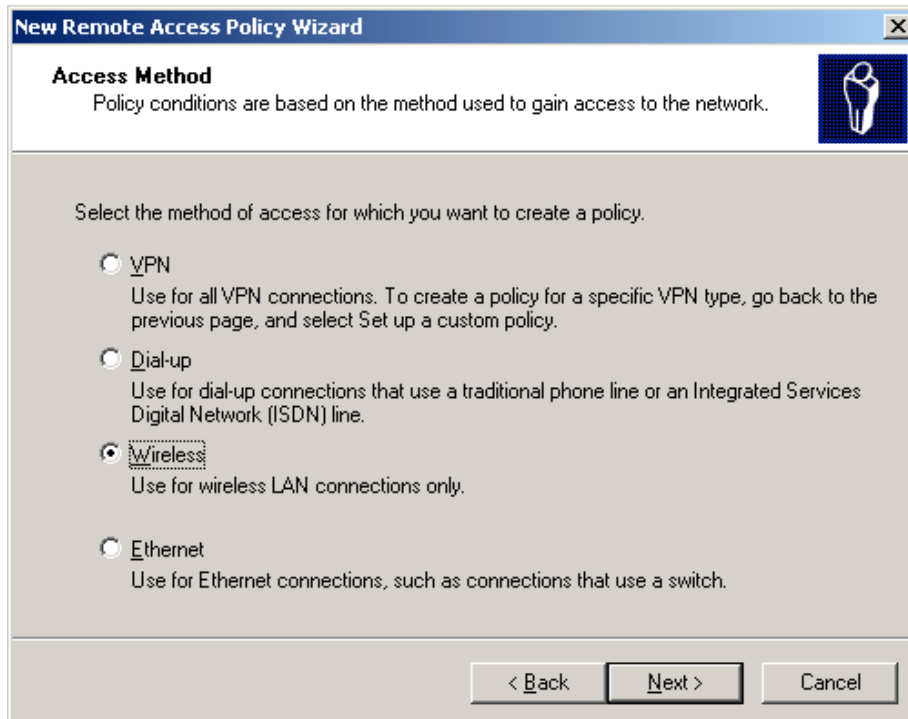
Type a name that describes this policy.

Policy name:

Example: Authenticate all VPN connections.

< Back Next > Cancel

Next select “Wireless” as the access method, and select “Next” to continue.



The screenshot shows the 'New Remote Access Policy Wizard' window, specifically the 'Access Method' step. The window has a title bar with the text 'New Remote Access Policy Wizard' and a close button. Below the title bar is a header section with the title 'Access Method' and a sub-header 'Policy conditions are based on the method used to gain access to the network.' To the right of the header is a small icon of a person. The main area of the window contains the question 'Select the method of access for which you want to create a policy.' followed by four radio button options: 'VPN' (with a description: 'Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.'), 'Dial-up' (with a description: 'Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.'), 'Wireless' (which is selected and has a description: 'Use for wireless LAN connections only.'), and 'Ethernet' (with a description: 'Use for Ethernet connections, such as connections that use a switch.'). At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

New Remote Access Policy Wizard

Access Method
Policy conditions are based on the method used to gain access to the network.

Select the method of access for which you want to create a policy.

☐ VPN
Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.

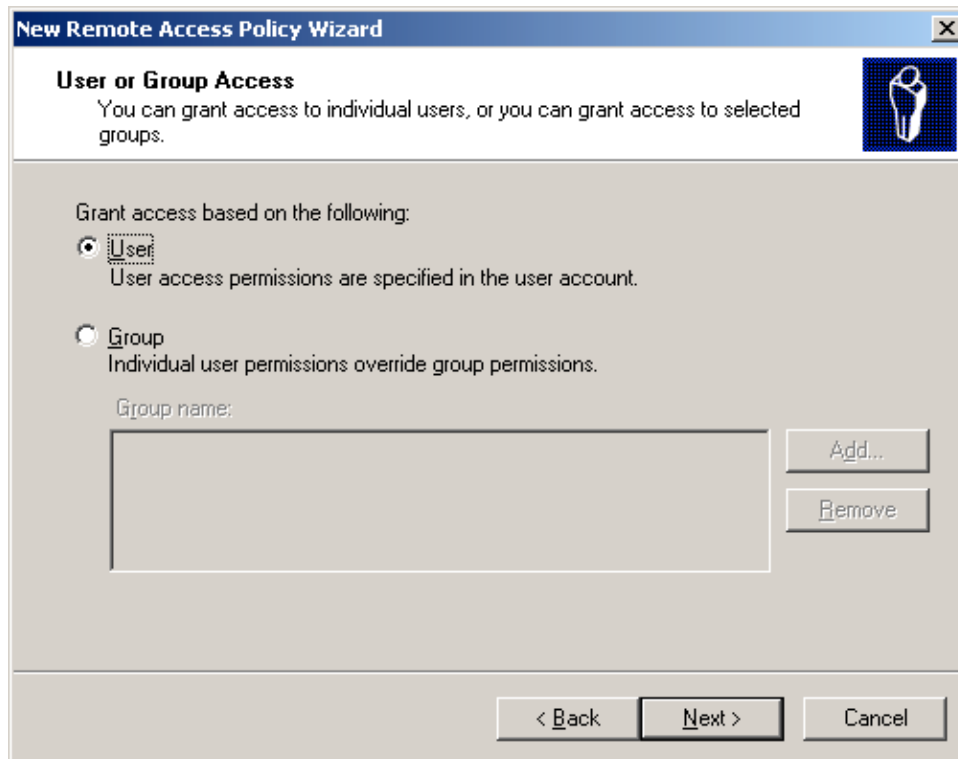
☐ Dial-up
Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.

☒ Wireless
Use for wireless LAN connections only.

☐ Ethernet
Use for Ethernet connections, such as connections that use a switch.

< Back Next > Cancel

Now you will be asked if you want to grant access by individual user or by groups. In the example below, User is chosen. Select "Next" to continue.



The screenshot shows the 'New Remote Access Policy Wizard' window, specifically the 'User or Group Access' step. The window has a title bar with the text 'New Remote Access Policy Wizard' and a close button. Below the title bar is a header area with the title 'User or Group Access' and a sub-header 'You can grant access to individual users, or you can grant access to selected groups.' To the right of the header is a small icon of a person. The main area of the window contains the text 'Grant access based on the following:' followed by two radio button options. The first option is 'User', which is selected, and its description is 'User access permissions are specified in the user account.' The second option is 'Group', and its description is 'Individual user permissions override group permissions.' Below the 'Group' option is a text box labeled 'Group name:' and two buttons, 'Add...' and 'Remove'. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

New Remote Access Policy Wizard

User or Group Access
You can grant access to individual users, or you can grant access to selected groups.

Grant access based on the following:

☒ **User**
User access permissions are specified in the user account.

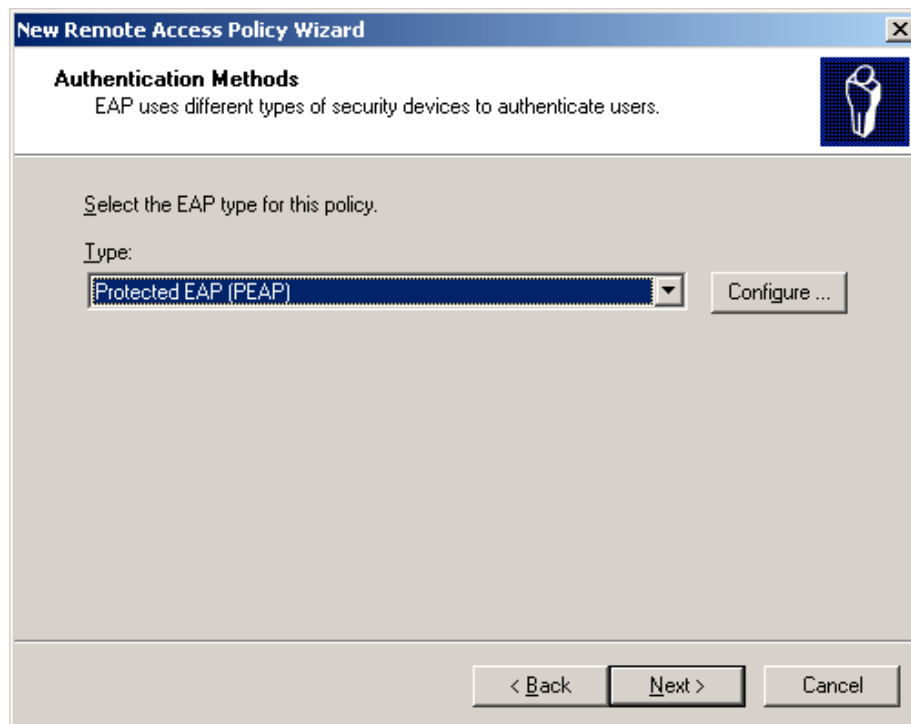
☐ **Group**
Individual user permissions override group permissions.

Group name:

Add...
Remove

< Back Next > Cancel

Now you will be asked what EAP type to use. IAS only supports PEAP and EAP-TLS. In this example PEAP is selected. Select "Next" to continue.



The screenshot shows the 'New Remote Access Policy Wizard' window, specifically the 'Authentication Methods' step. The window has a title bar with the text 'New Remote Access Policy Wizard' and a close button. Below the title bar is a header area with the title 'Authentication Methods' and a sub-header 'EAP uses different types of security devices to authenticate users.' To the right of the header is a small icon of a person. The main area of the window contains the text 'Select the EAP type for this policy.' followed by a label 'Type:' and a dropdown menu. The dropdown menu is currently set to 'Protected EAP (PEAP)'. To the right of the dropdown menu is a button labeled 'Configure ...'. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

New Remote Access Policy Wizard

Authentication Methods
EAP uses different types of security devices to authenticate users.

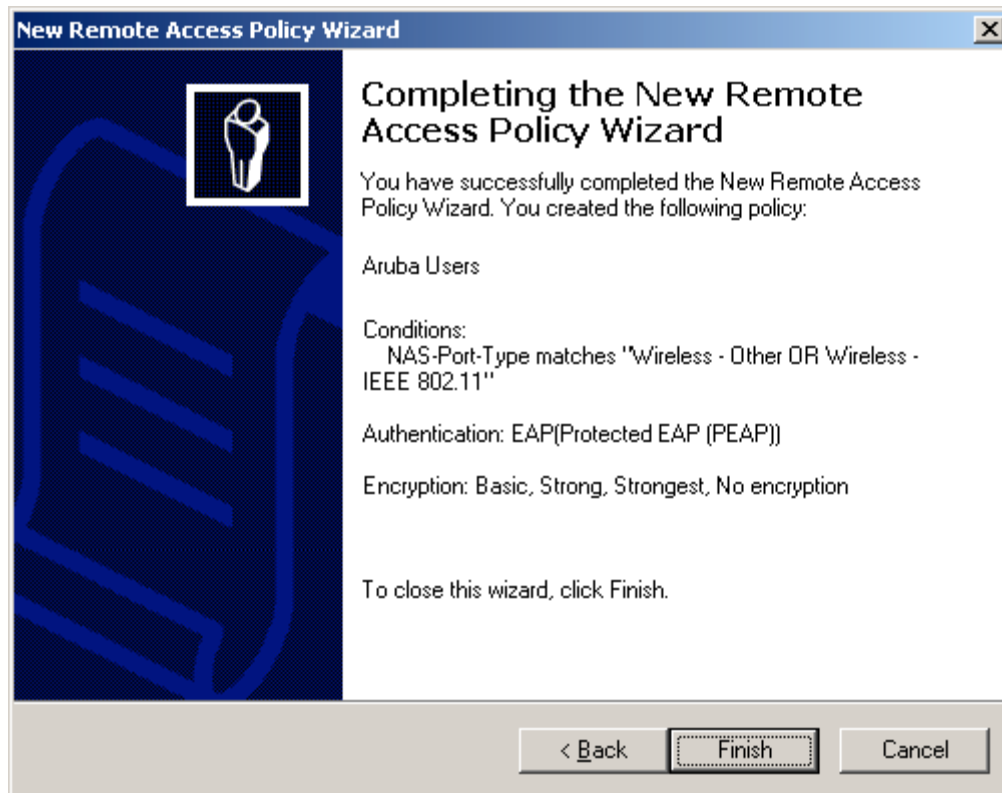
Select the EAP type for this policy.

Type:

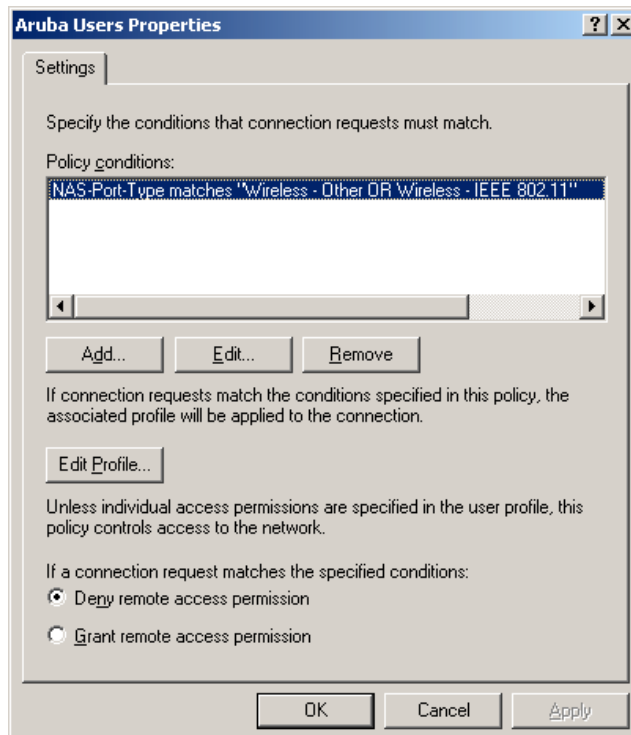
Protected EAP (PEAP) Configure ...

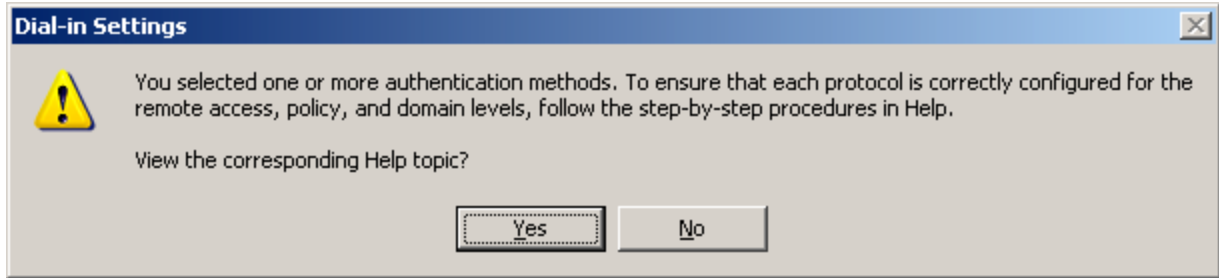
< Back Next > Cancel

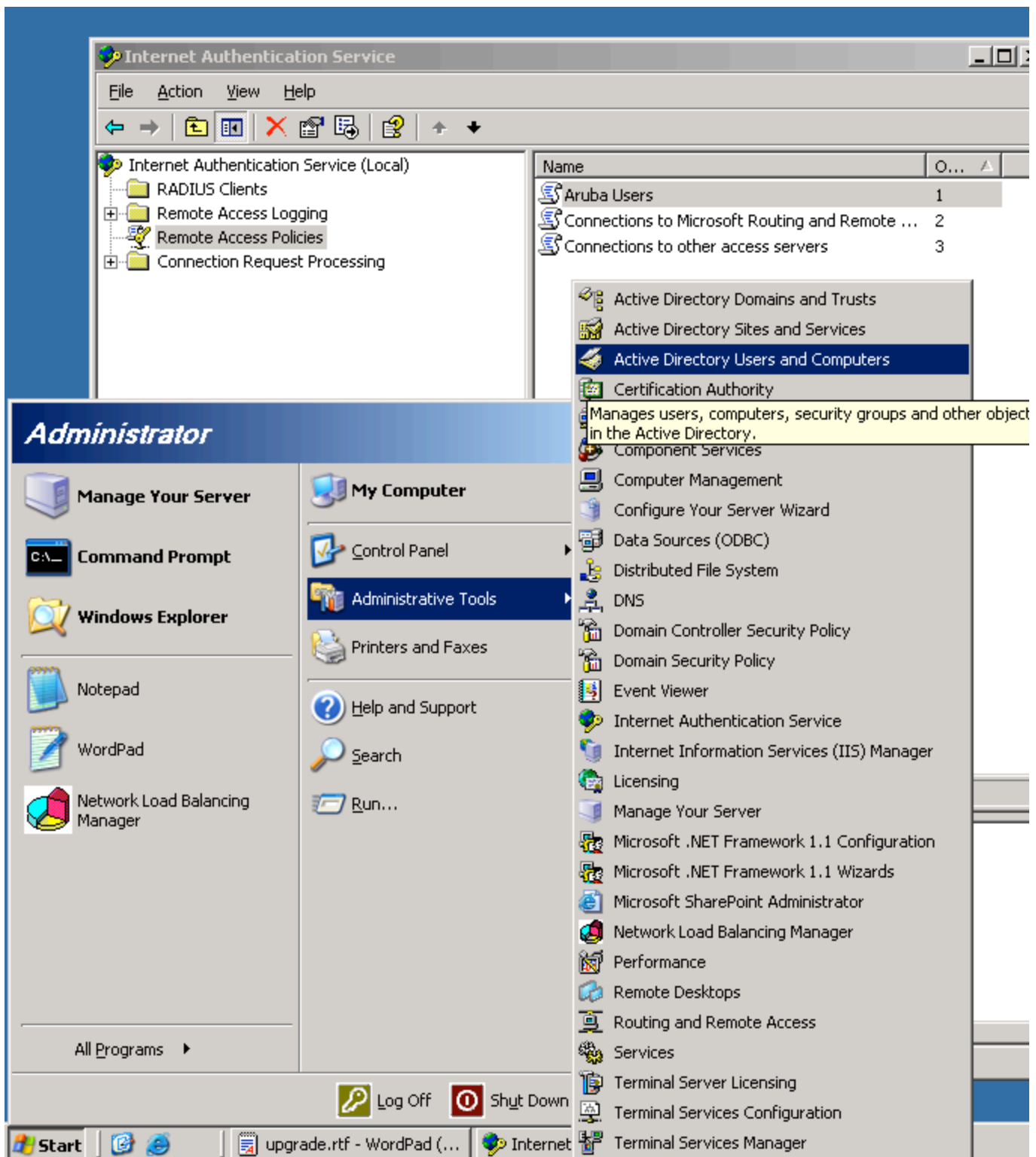
The following window will be displayed. Select "Finish".

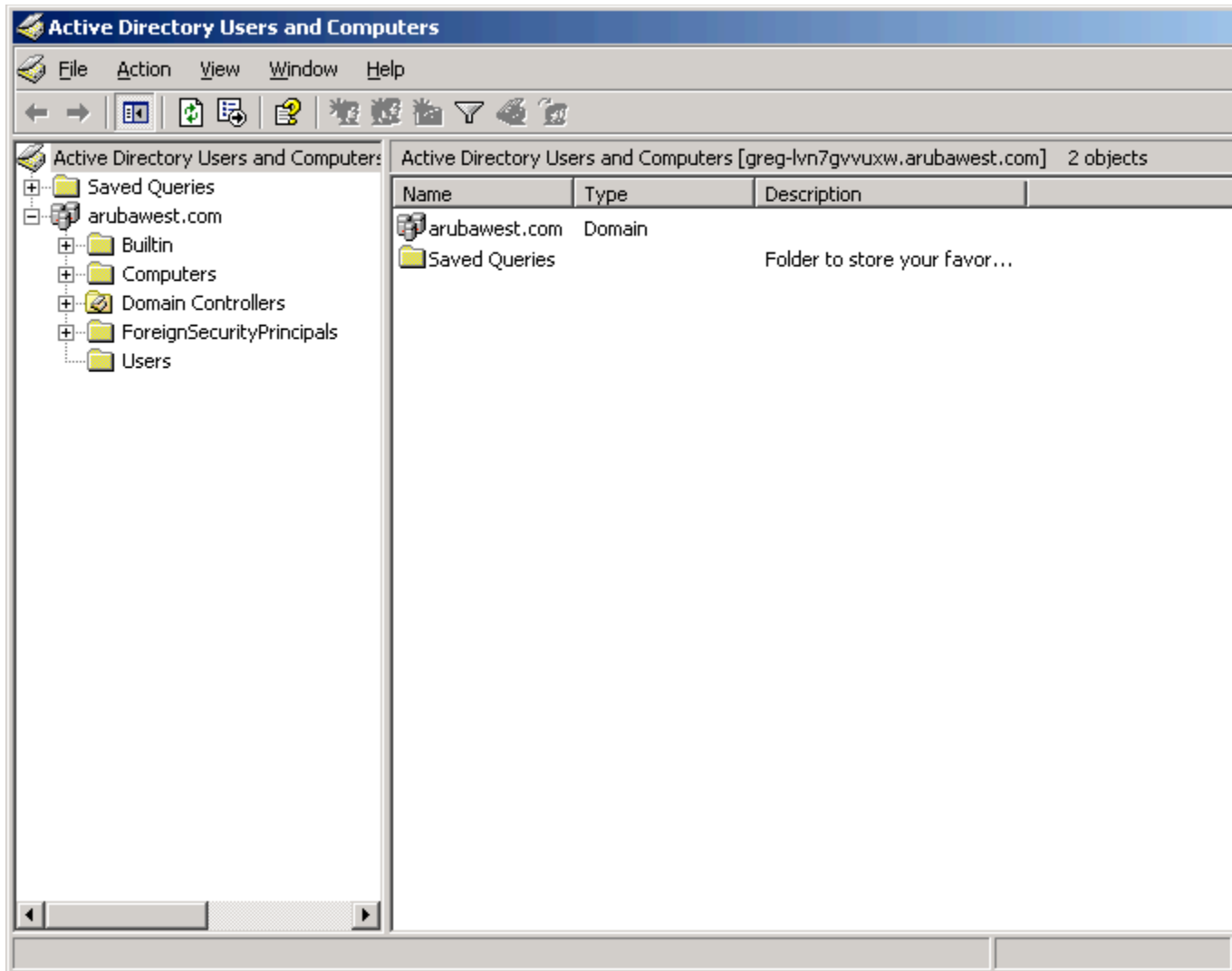


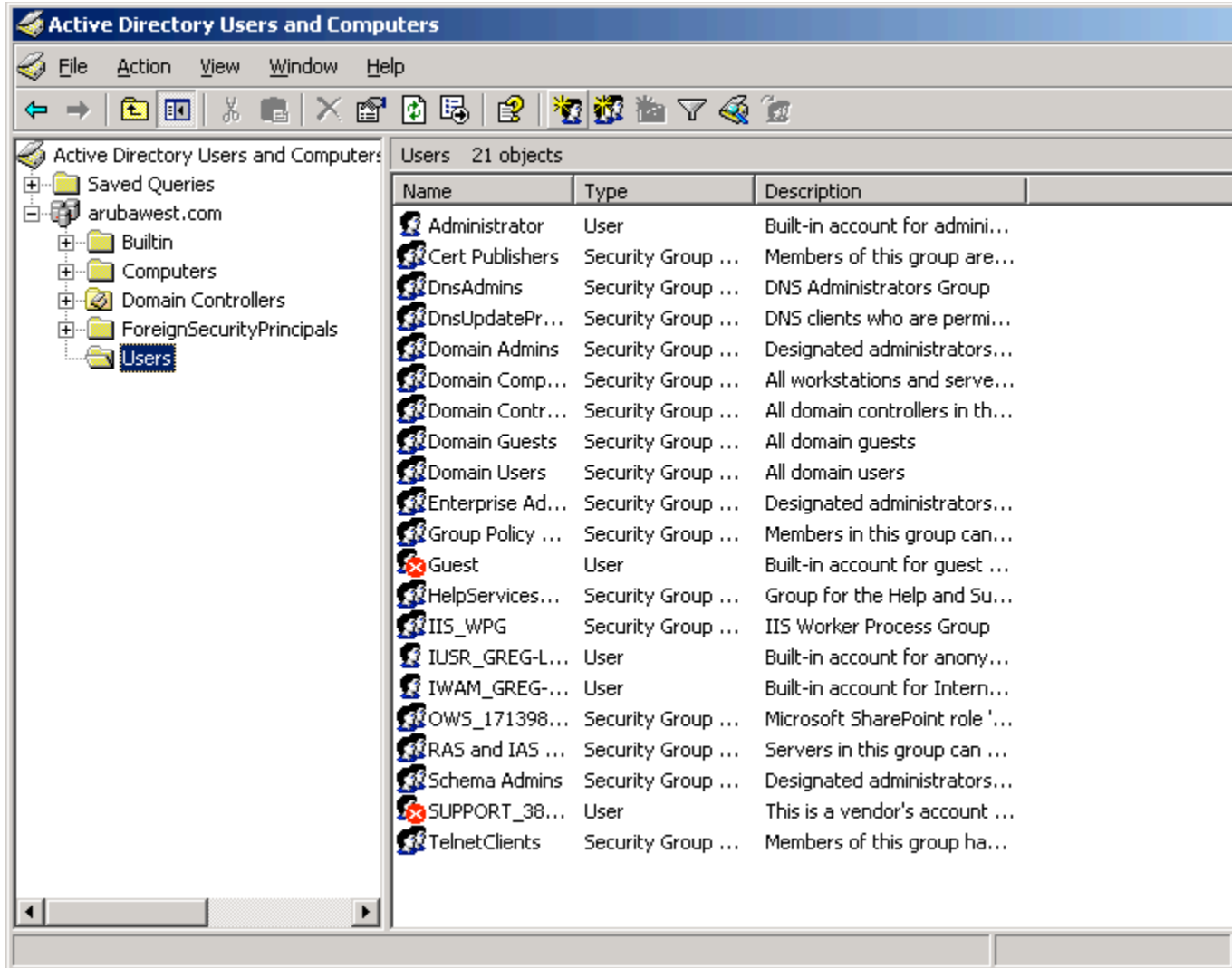
The new policy will be added











New Object - User

Create in: arubawest.com/Users

Password:

Confirm password:

☐ User must change password at next logon

☐ User cannot change password

☒ Password never expires

☐ Account is disabled

< Back Next > Cancel

New Object - User

Create in: arubawest.com/Users

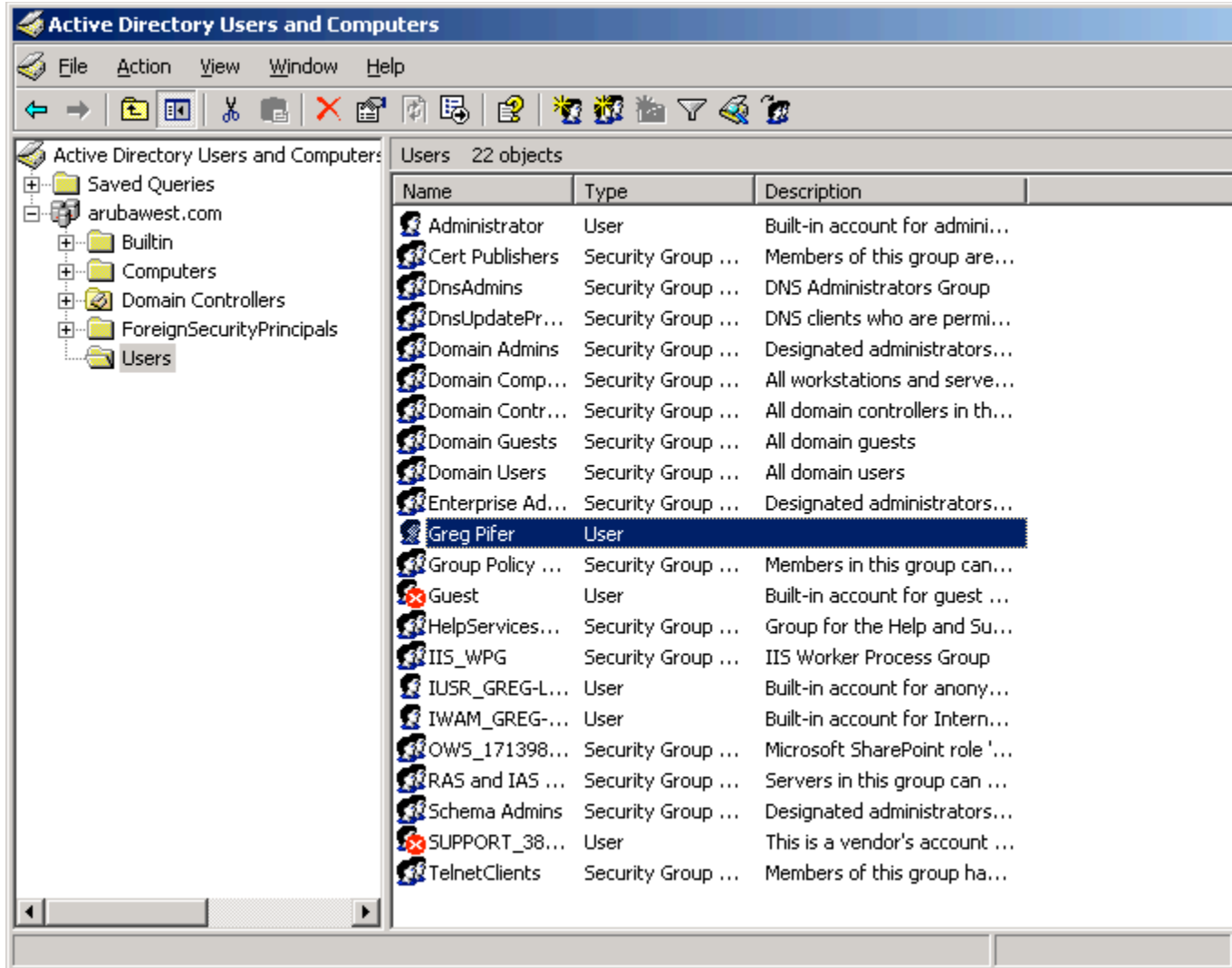
When you click Finish, the following object will be created:

Full name: Greg Pifer

User logon name: gpifer@arubawest.com

The password never expires.

< Back Finish Cancel



Greg Pifer Properties [?] [X]

Remote control		Terminal Services Profile		COM+	
General	Address	Account	Profile	Telephones	Organization
Member Of		Dial-in	Environment		Sessions

Remote Access Permission (Dial-in or VPN)

☒ Allow access

☐ Deny access

☐ Control access through Remote Access Policy

☐ Verify Caller-ID:

Callback Options

☒ No Callback

☐ Set by Caller (Routing and Remote Access Service only)

☐ Always Callback to:

☐ Assign a Static IP Address

☐ Apply Static Routes

Define routes to enable for this Dial-in connection.

[OK] [Cancel] [Apply]