

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 screenshot shows the 'Manage Your Server' console window. The title bar reads 'Manage Your Server'. The main header area contains a server icon, the text 'Manage Your Server', and 'Server: GREG-LVN7GVUJXW'. To the right is a search box for the 'Help and Support Center' with a green arrow button. The main content area is divided into two columns. The left column has two sections: 'Adding Roles to Your Server' with a server icon and a description, and 'Managing Your Server Roles' with a server icon and a description. The right column has two sections: 'Tools and Updates' with a list of links including 'Administrative Tools', 'More Tools', 'Windows Update', 'Computer and Domain Name Information', and 'Internet Explorer Enhanced Security Configuration'; and 'See Also' with a list of links including 'Help and Support', 'Microsoft TechNet', 'Deployment and Resource Kits', 'List of Common Administrative Tasks', 'Windows Server Communities', 'What's New', and 'Strategic Technology Protection Program'. At the bottom left, there is a checkbox labeled 'Don't display this page at logon'.

Manage Your Server
Server: GREG-LVN7GVUJXW

Adding Roles to Your Server
Adding roles to your server lets it perform specific tasks. For example, the file server role enables your server to share files. To add a role, start the Configure Your Server Wizard by clicking Add or remove a role.

- Add or remove a role
- Read about server roles

Managing Your Server Roles
After you have added a role, return to this page at any time for tools and information to help you with your daily administrative tasks.

No roles have been added to this server. To add a role, click Add or remove a role.

Tools and Updates

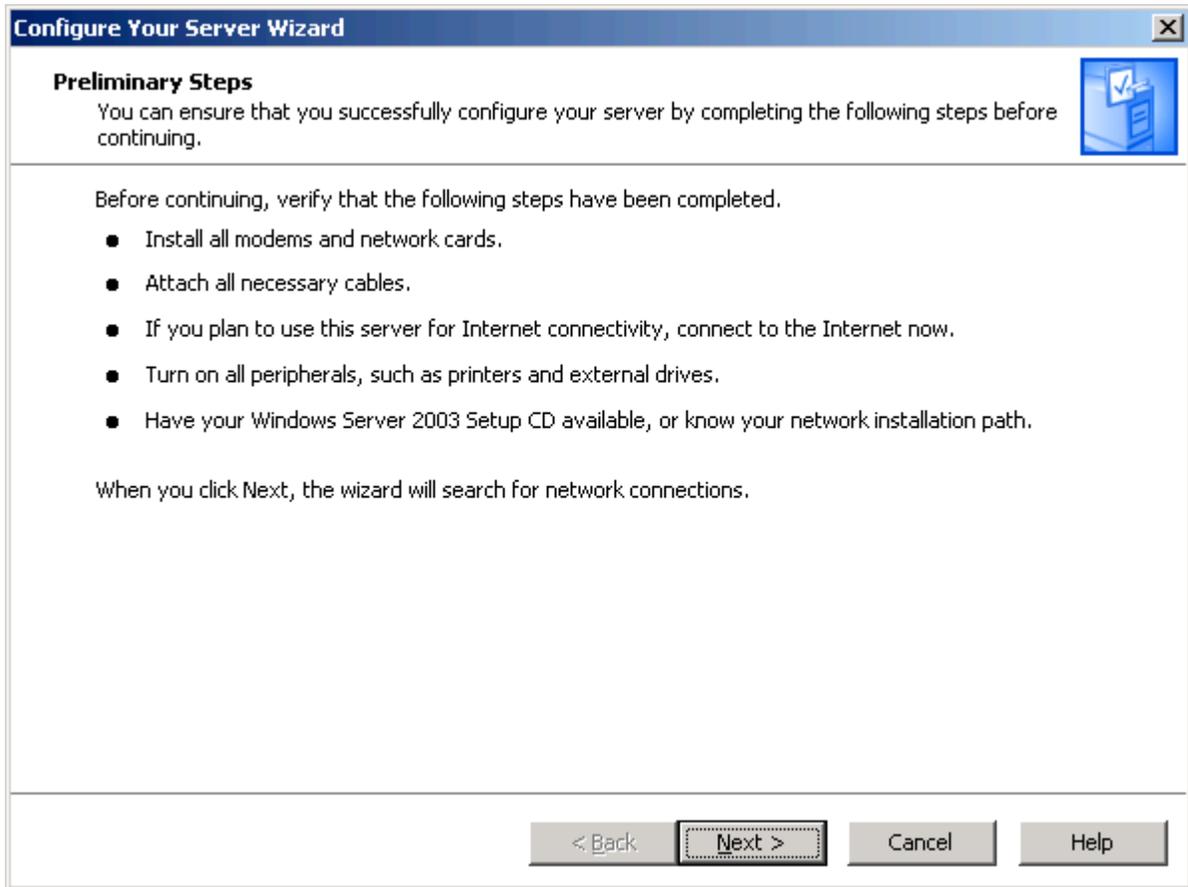
- Administrative Tools
- More Tools
- Windows Update
- Computer and Domain Name Information
- Internet Explorer Enhanced Security Configuration

See Also

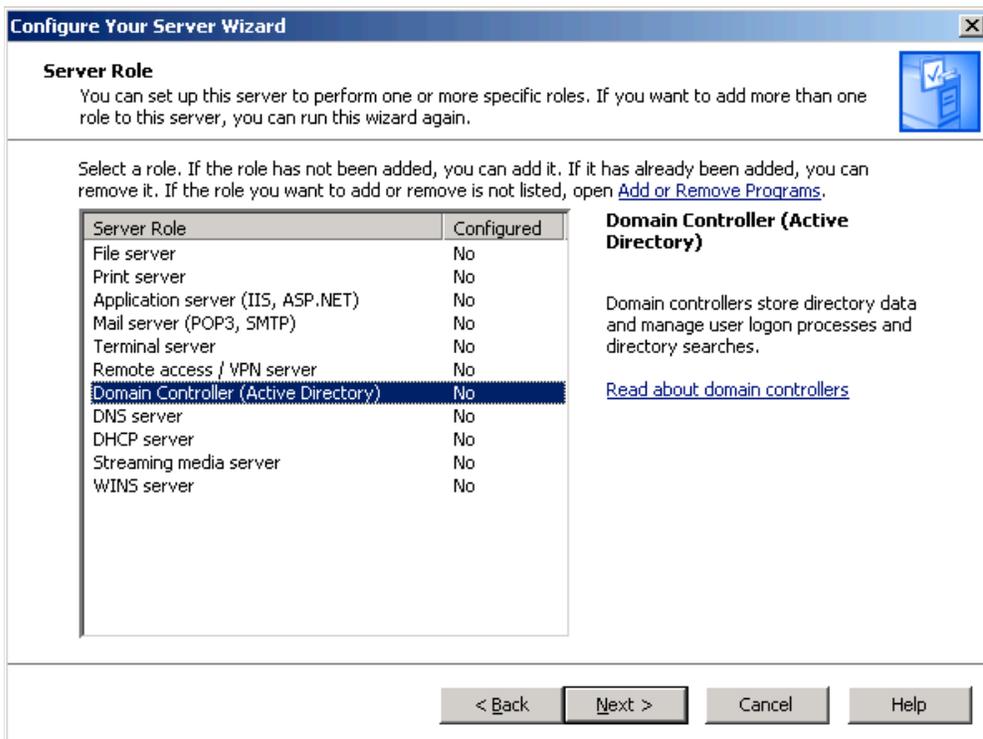
- Help and Support
- Microsoft TechNet
- Deployment and Resource Kits
- List of Common Administrative Tasks
- Windows Server Communities
- What's New
- Strategic Technology Protection Program

Don't display this page at logon

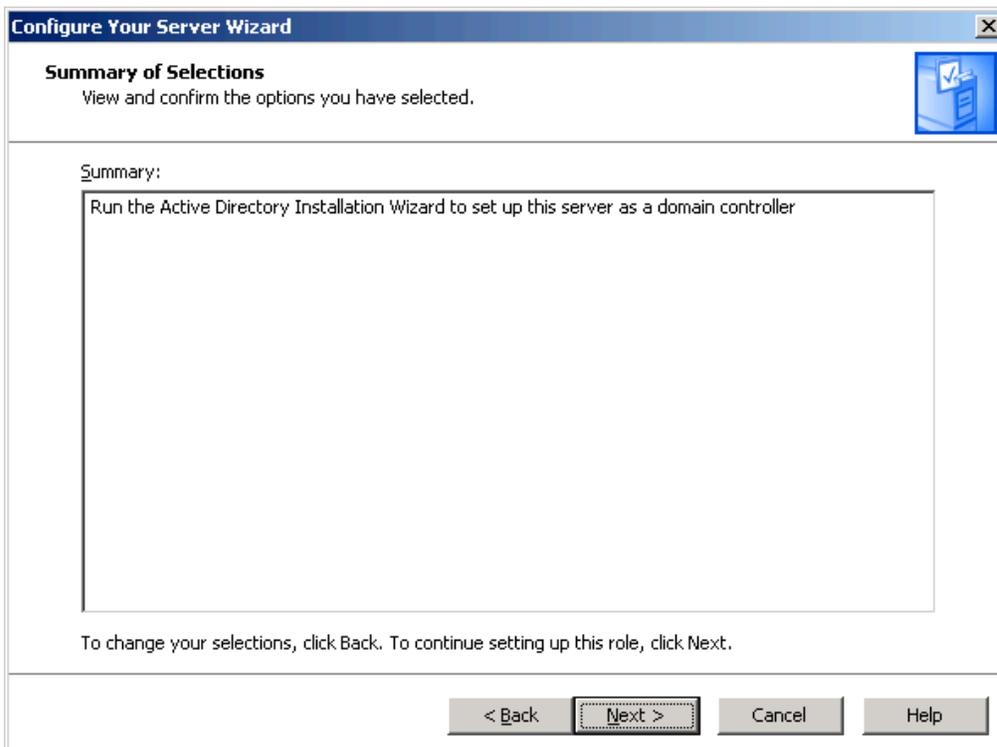
The configuration wizard will now start and ask you to verify that preliminary steps have been completed. Hit "Next" to continue.



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.



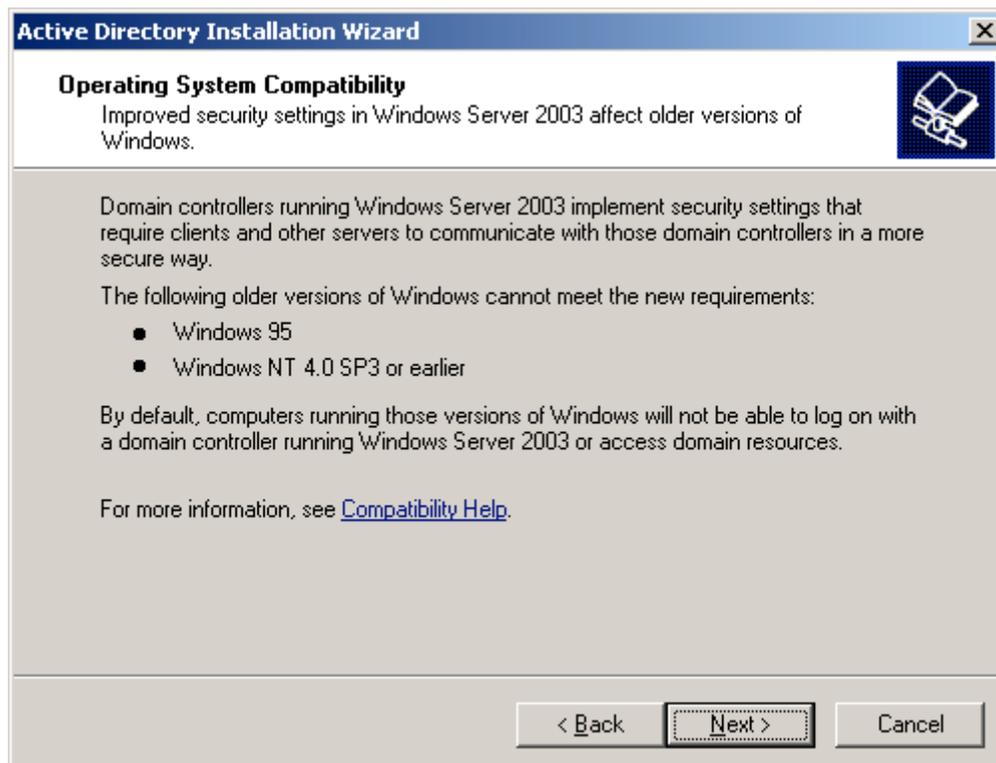
The Wizard will ask you to confirm your selection. Press “Next” to confirm and continue.



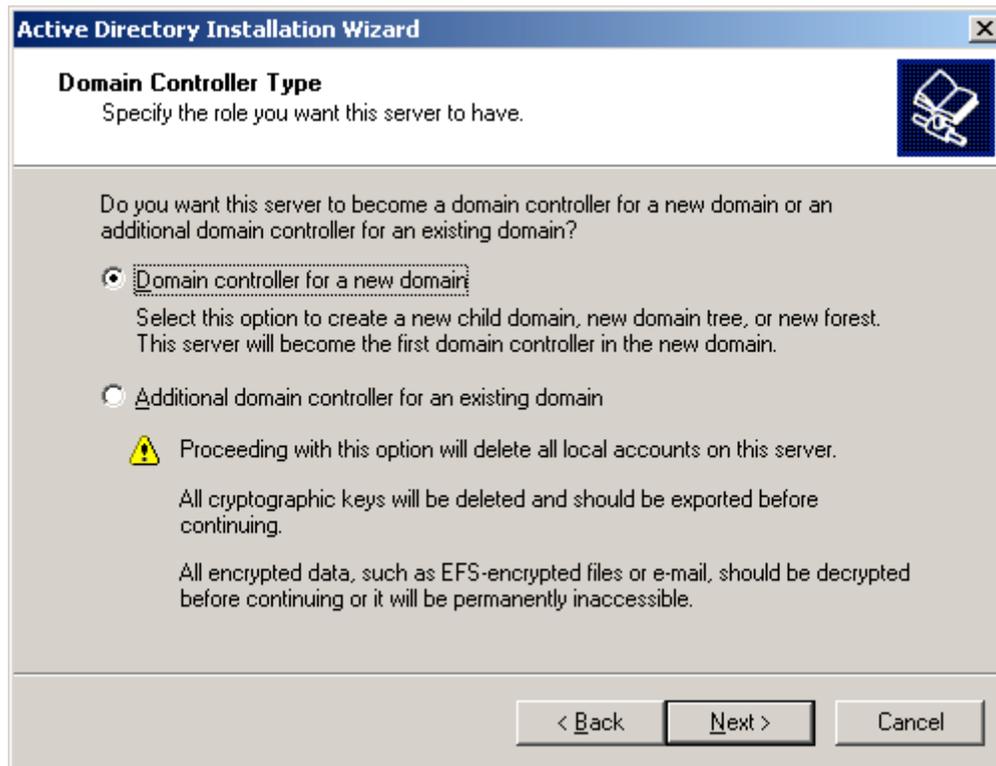
The Active Directory Installation Wizard will now start. Select "Next" to continue.



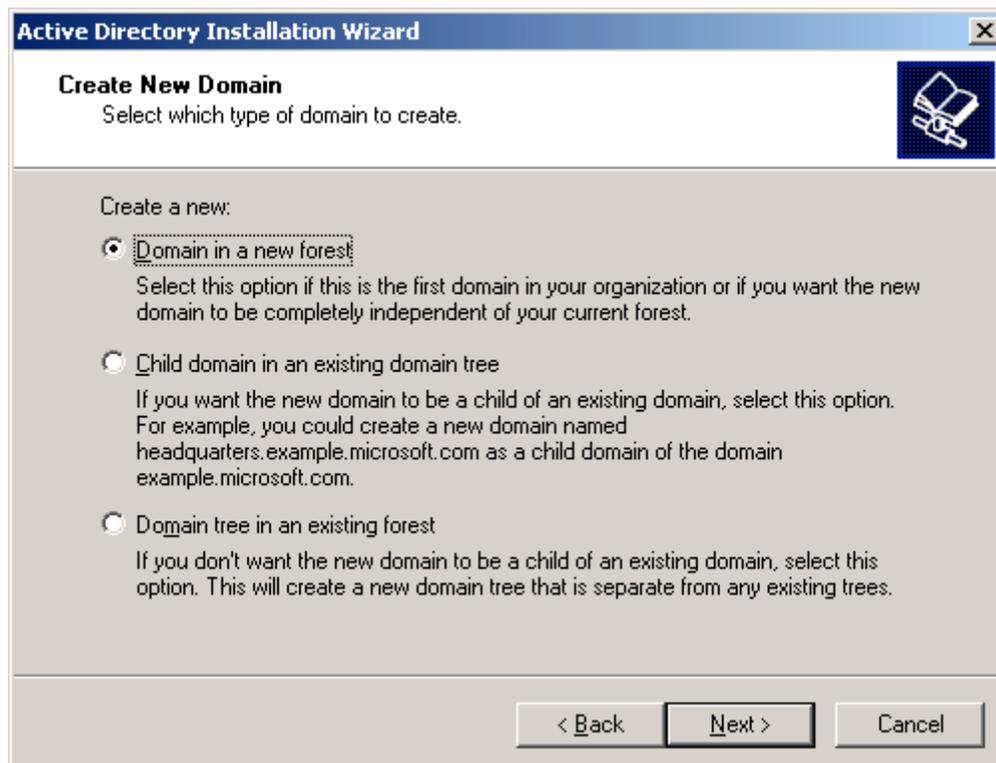
A warning window will now be displayed. Press "Next" to continue.



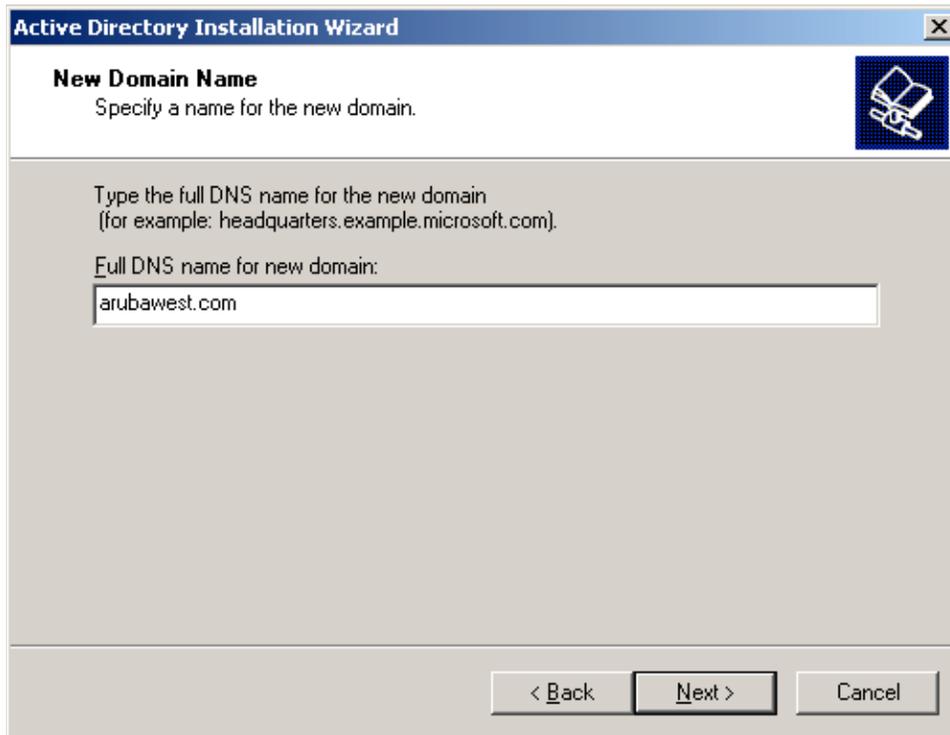
You will now be asked to specify a Domain Controller Type. Here we will want to select the Domain controller for a new domain radio button, and select “Next” to continue.



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

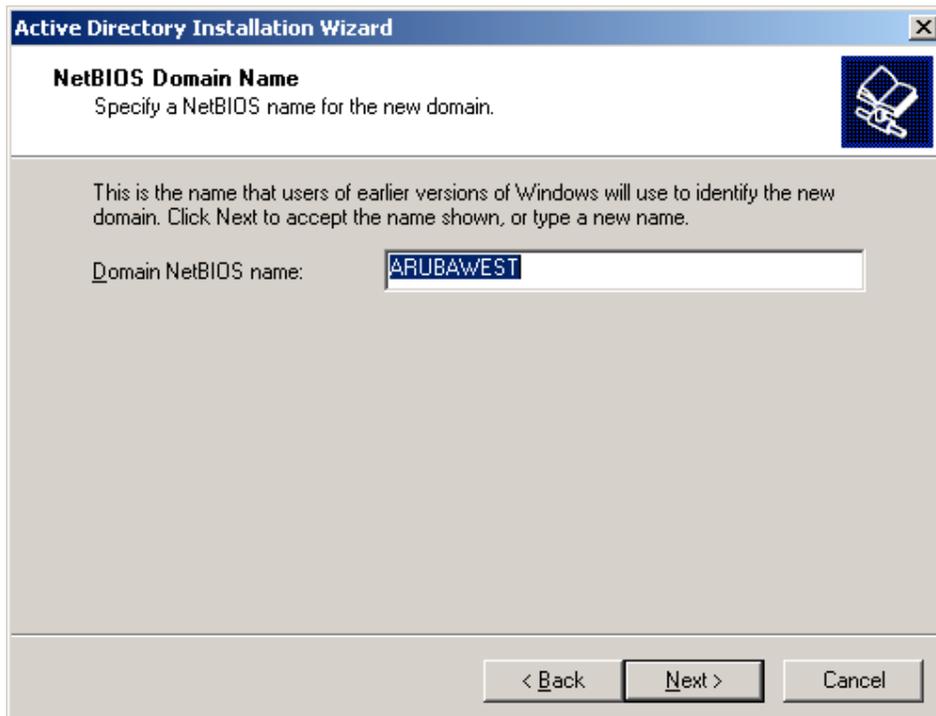


At this point you will be asked for the DNS name of the new domain to be created. Enter the desired domain name and select “Next” to continue.



The screenshot shows the 'Active Directory Installation Wizard' window. The title bar reads 'Active Directory Installation Wizard'. The main heading is 'New Domain Name' with a sub-instruction: 'Specify a name for the new domain.' Below this, there is a text box containing 'arubawest.com'. The text above the text box says: 'Type the full DNS name for the new domain (for example: headquarters.example.microsoft.com). Full DNS name for new domain:'. At the bottom of the window are three buttons: '< Back', 'Next >', and '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 reads 'Active Directory Installation Wizard'. The main heading is 'NetBIOS Domain Name' with a sub-instruction: 'Specify a NetBIOS name for the new domain.' Below this, there is a text box containing 'ARUBAWEST'. The text above the text box says: '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.' Below the text box is the label 'Domain NetBIOS name:'. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

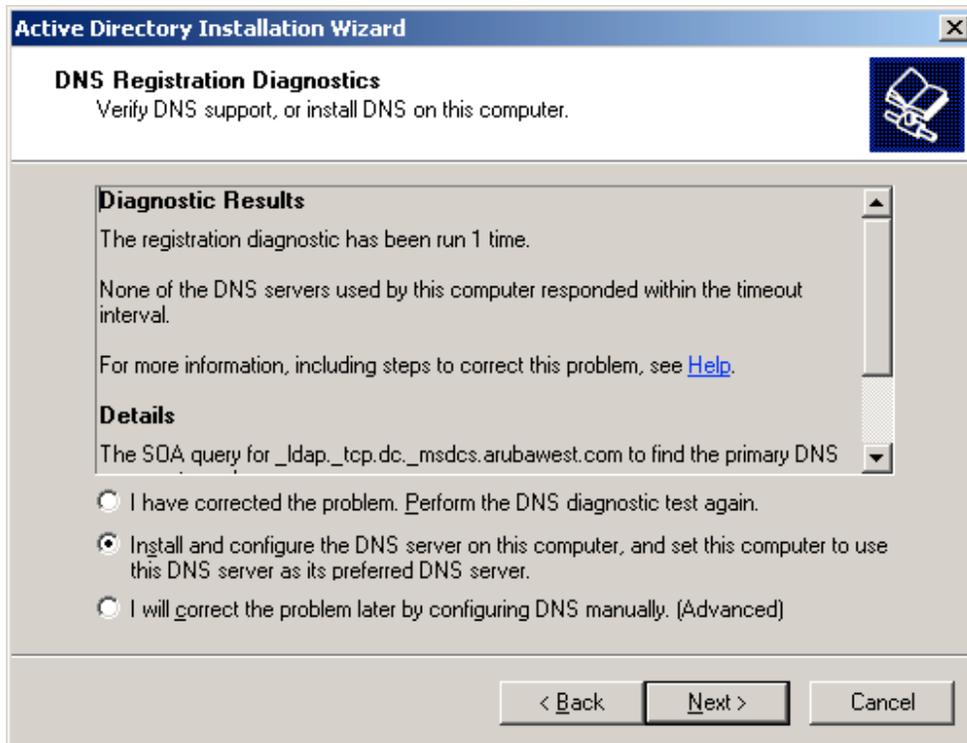
Now you will be given the option to change the location of the Active Directory database and directory. Just keep the defaults and select “Next” to continue.

The screenshot shows the 'Active Directory Installation Wizard' window. 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, there is a note: 'For best performance and recoverability, store the database and the log on separate hard disks.' The question is 'Where do you want to store the Active Directory database?'. The 'Database folder:' label is followed by a text box containing 'C:\WINDOWS\NTDS' and a 'Browse...' button. The second question is 'Where do you want to store the Active Directory log?'. The 'Log folder:' label is followed by a text box containing 'C:\WINDOWS\NTDS' and a 'Browse...' button. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

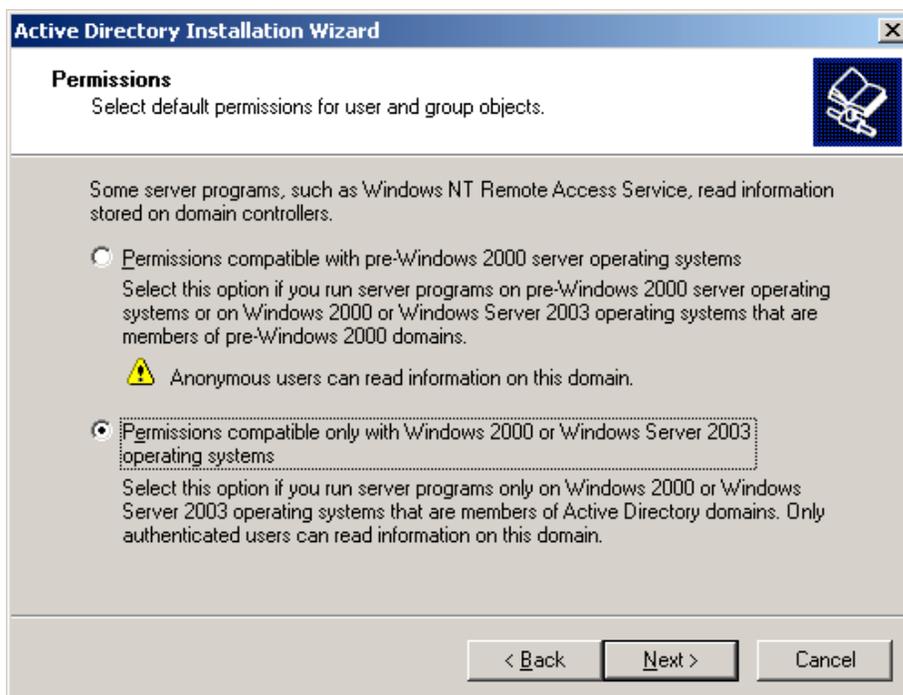
Now you can change the location of the Shared System Volume. Select “Next” to continue.

The screenshot shows the 'Active Directory Installation Wizard' window. 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, there is a note: '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 is 'Enter a location for the SYSVOL folder.' The 'Folder location:' label is followed by a text box containing 'C:\WINDOWS\SYSVOL' and a 'Browse...' button. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

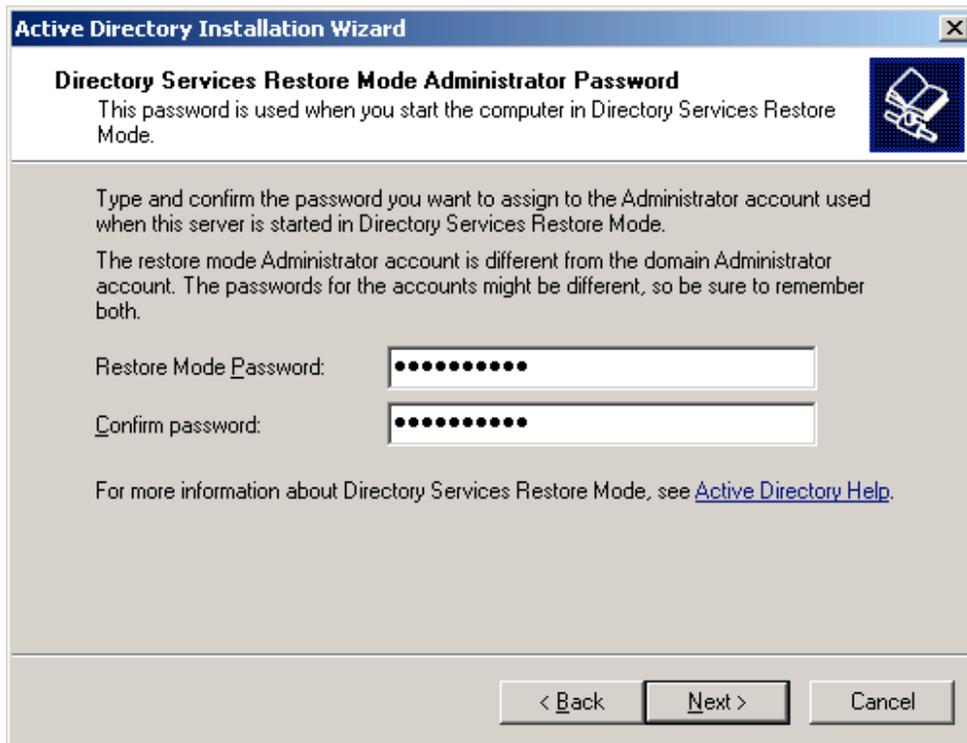
At this point the wizard will give you the option of installing DNS on this server. If you ever want to add a computer to this domain, it will be necessary for that computer to have access to the DNS for this domain. Since this is a fictitious domain, it works best if this server also acts as the DNS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

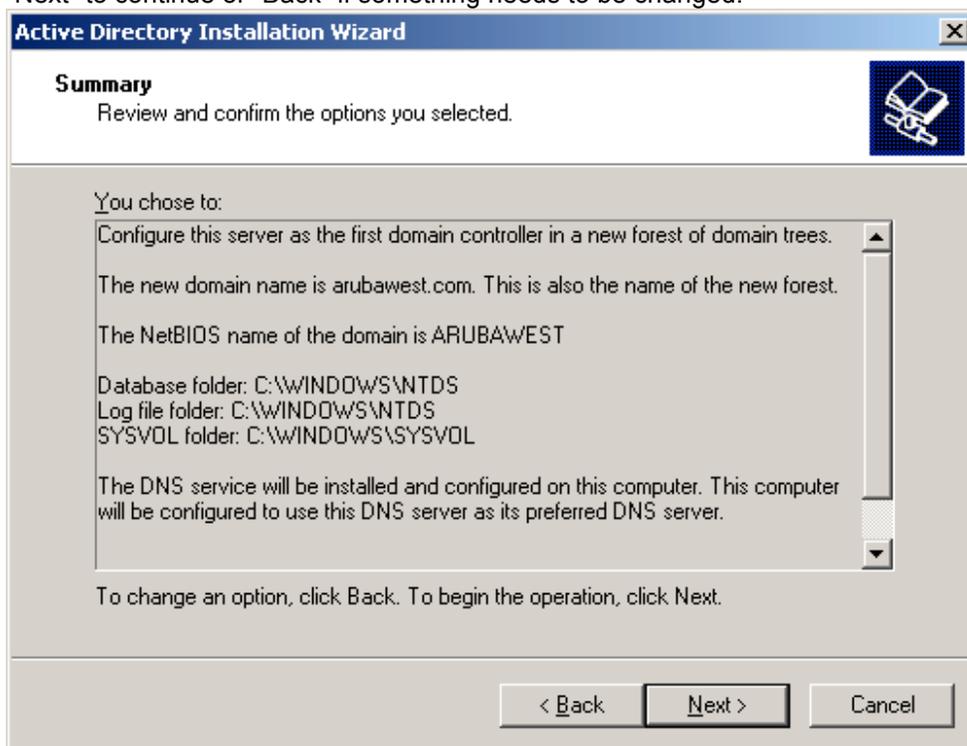
Restore Mode Password:

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 ARUBAWEST

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.

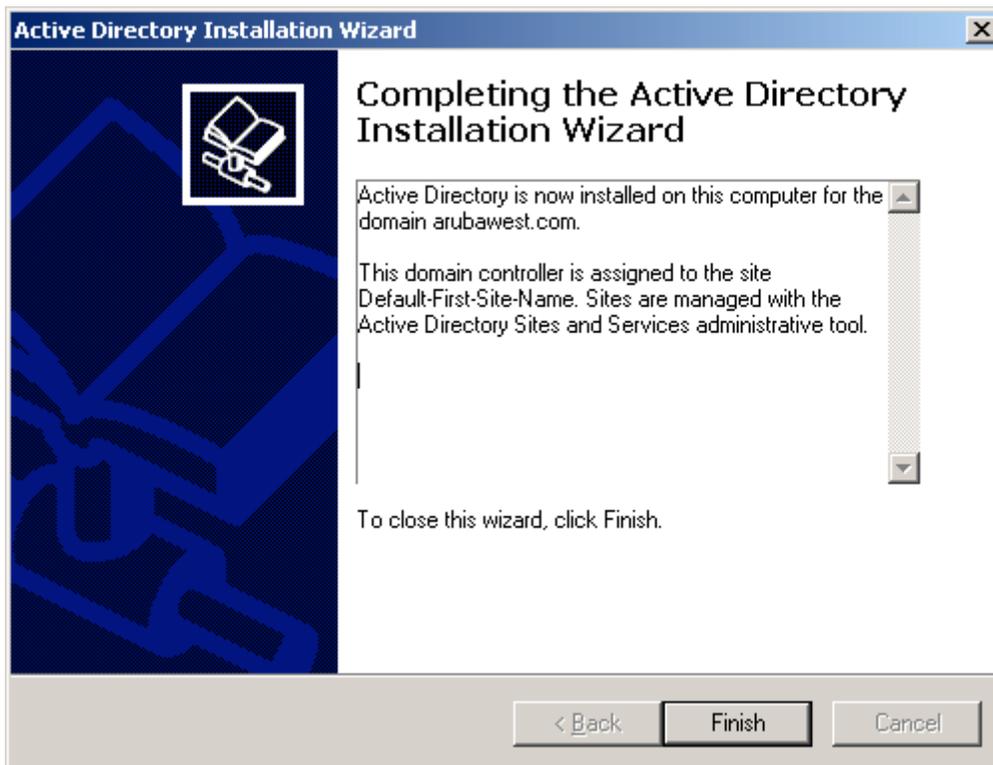
To change an option, click Back. To begin the operation, click Next.

< Back Next > Cancel

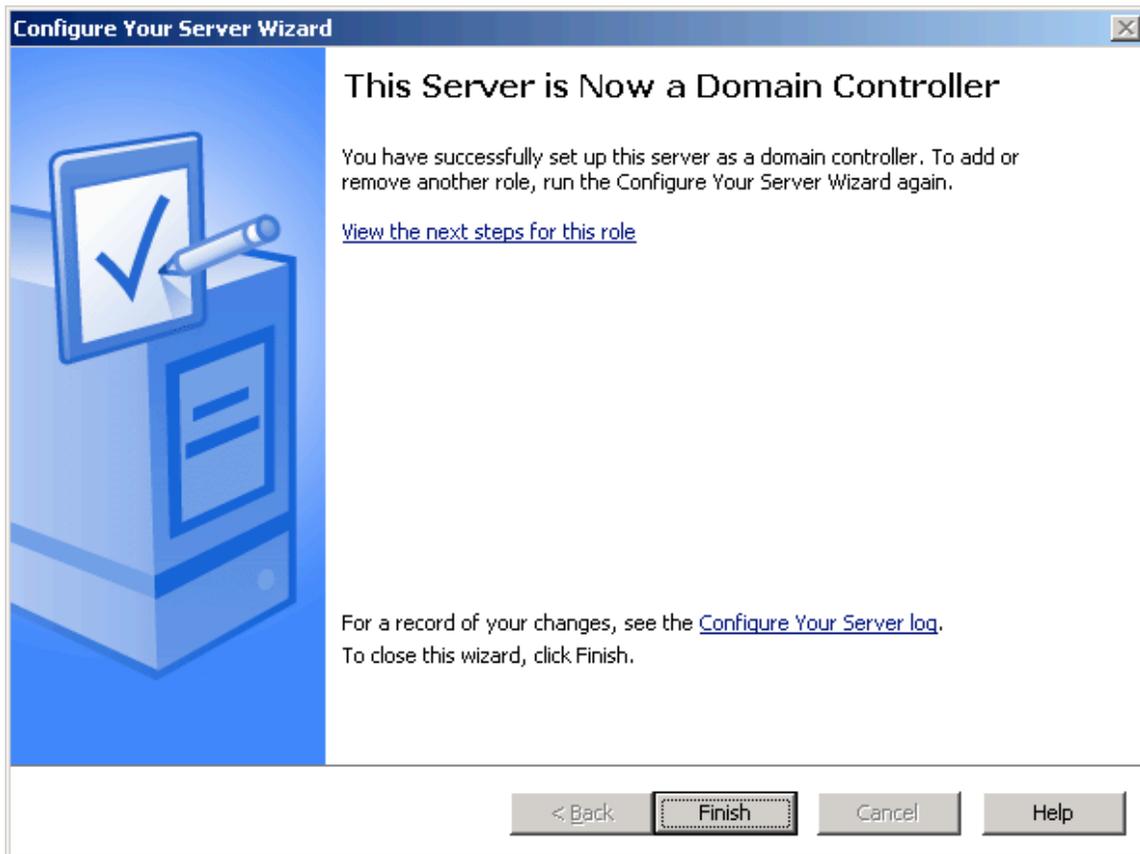
At this point the Active Directory Installation Wizard will install and configure AD based on all of your previous selections. This could take several minutes to complete.



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.

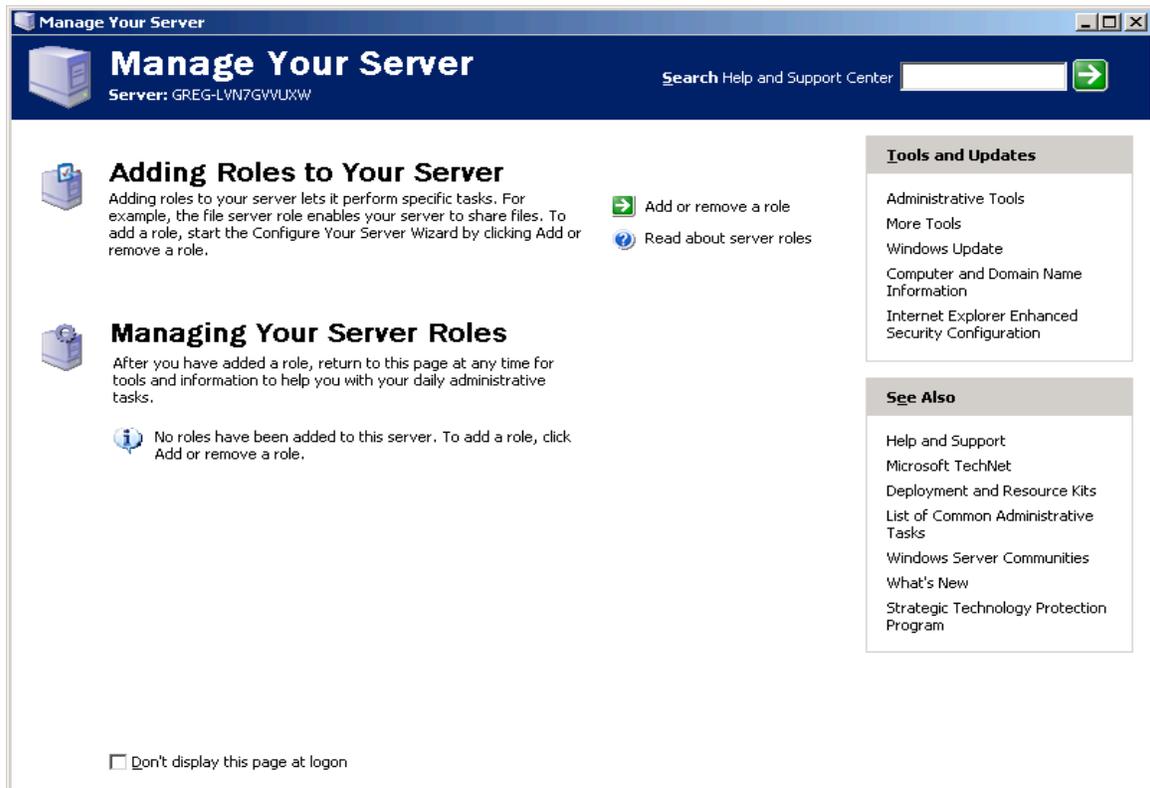


At this point you must restart the system. Select "Restart Now" and the server will reboot.



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.



The screenshot shows the 'Manage Your Server' console window. The title bar reads 'Manage Your Server'. The main header area contains the 'Manage Your Server' logo and the server name 'Server: GREG-LVN7GWLXW'. To the right of the header is a search bar for the 'Help and Support Center' with a green arrow button.

The main content area is divided into two columns. The left column contains two sections:

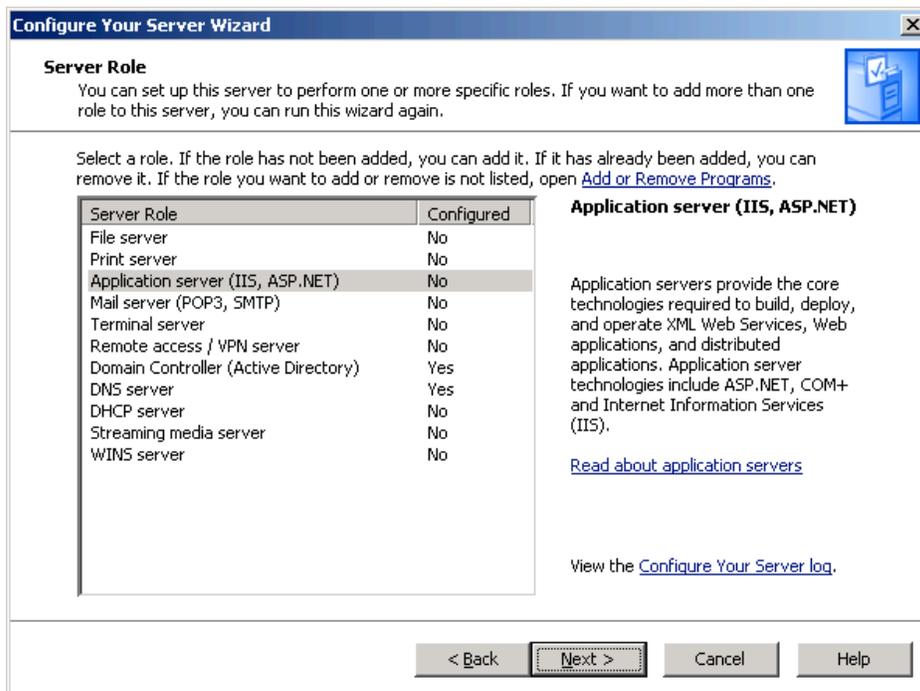
- Adding Roles to Your Server**: Accompanied by a server icon. The text reads: "Adding roles to your server lets it perform specific tasks. For example, the file server role enables your server to share files. To add a role, start the Configure Your Server Wizard by clicking Add or remove a role." To the right of this text are two links: "Add or remove a role" (with a green arrow icon) and "Read about server roles" (with a blue information icon).
- Managing Your Server Roles**: Accompanied by a server icon. The text reads: "After you have added a role, return to this page at any time for tools and information to help you with your daily administrative tasks." Below this is an information icon and the text: "No roles have been added to this server. To add a role, click Add or remove a role."

The right column contains two sections:

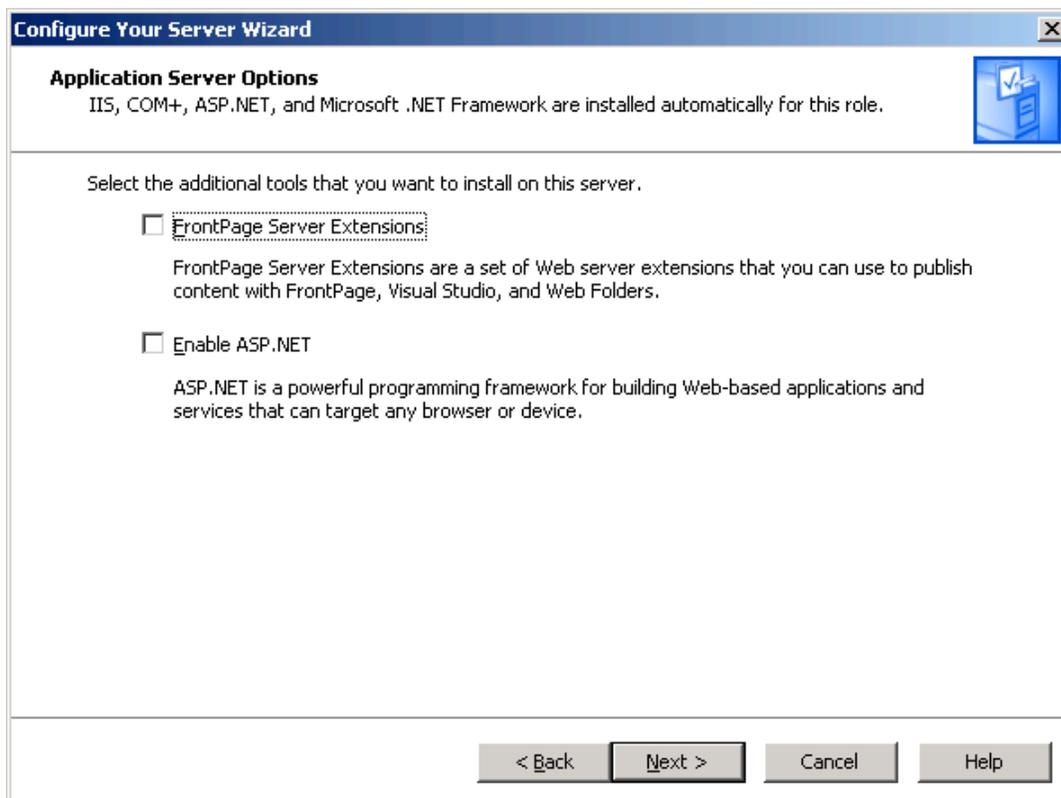
- Tools and Updates**: A list of links including "Administrative Tools", "More Tools", "Windows Update", "Computer and Domain Name Information", and "Internet Explorer Enhanced Security Configuration".
- See Also**: A list of links including "Help and Support", "Microsoft TechNet", "Deployment and Resource Kits", "List of Common Administrative Tasks", "Windows Server Communities", "What's New", and "Strategic Technology Protection Program".

At the bottom left of the window, there is a checkbox labeled "Don't display this page at logon".

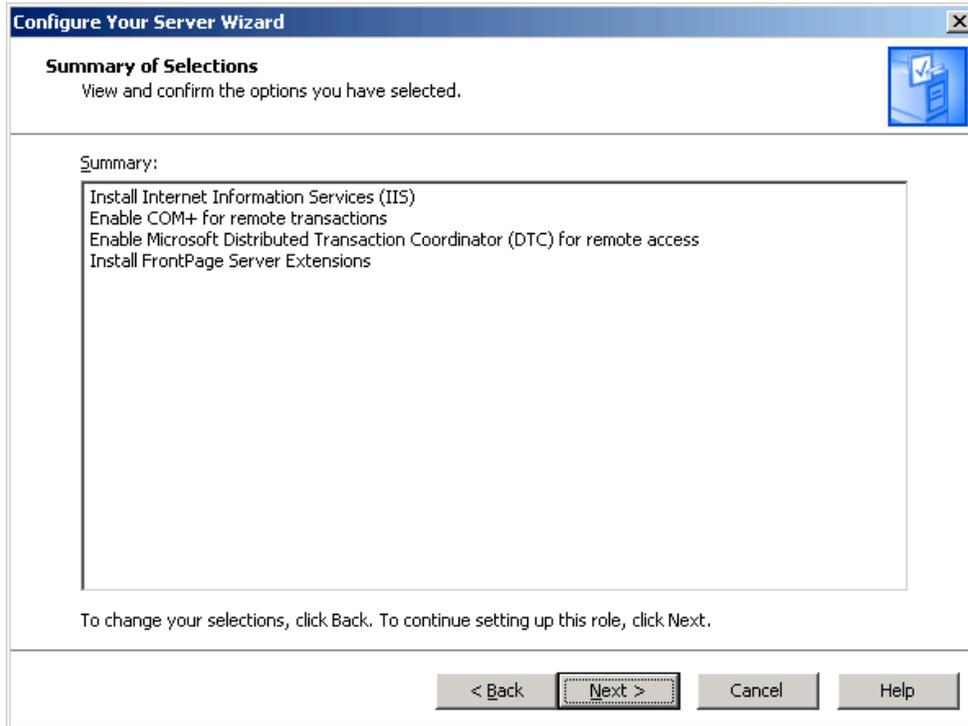
Now select “Application server(IIS, ASP.NET)” and select “Next” to continue.



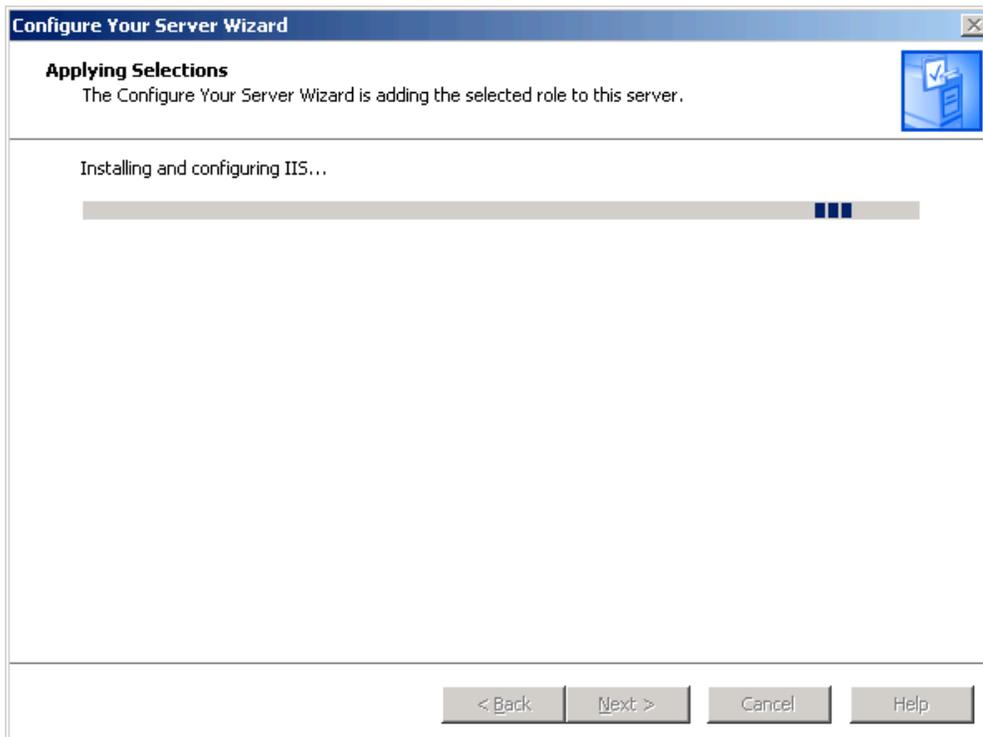
You will then be asked if you want to install any other tools on the server. You don't need any of these, so just select “Next” to continue.



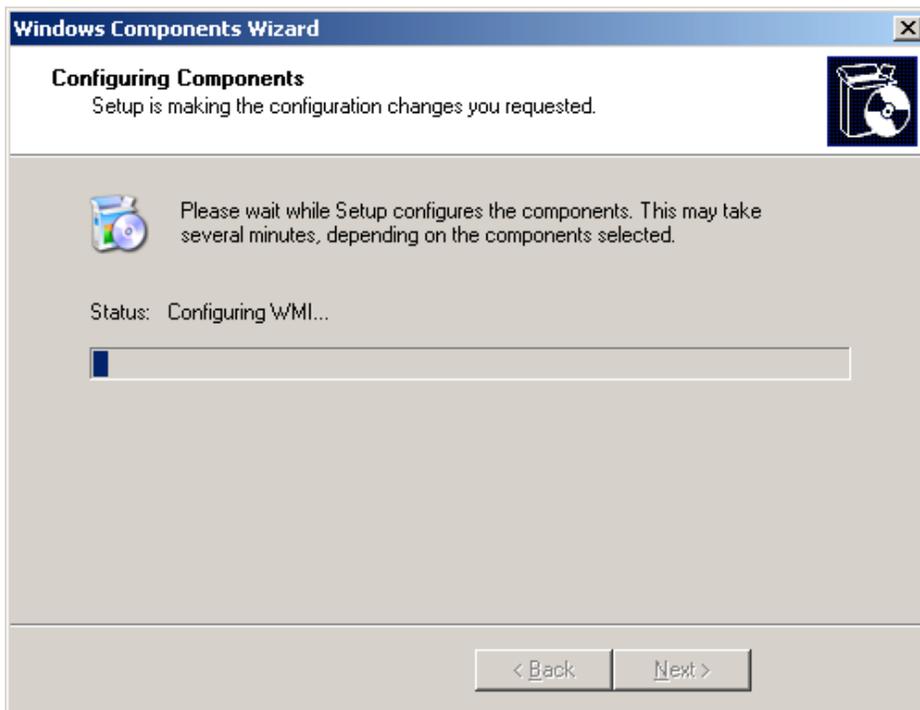
You will now have an opportunity to review your selections. Select "Next" to continue.



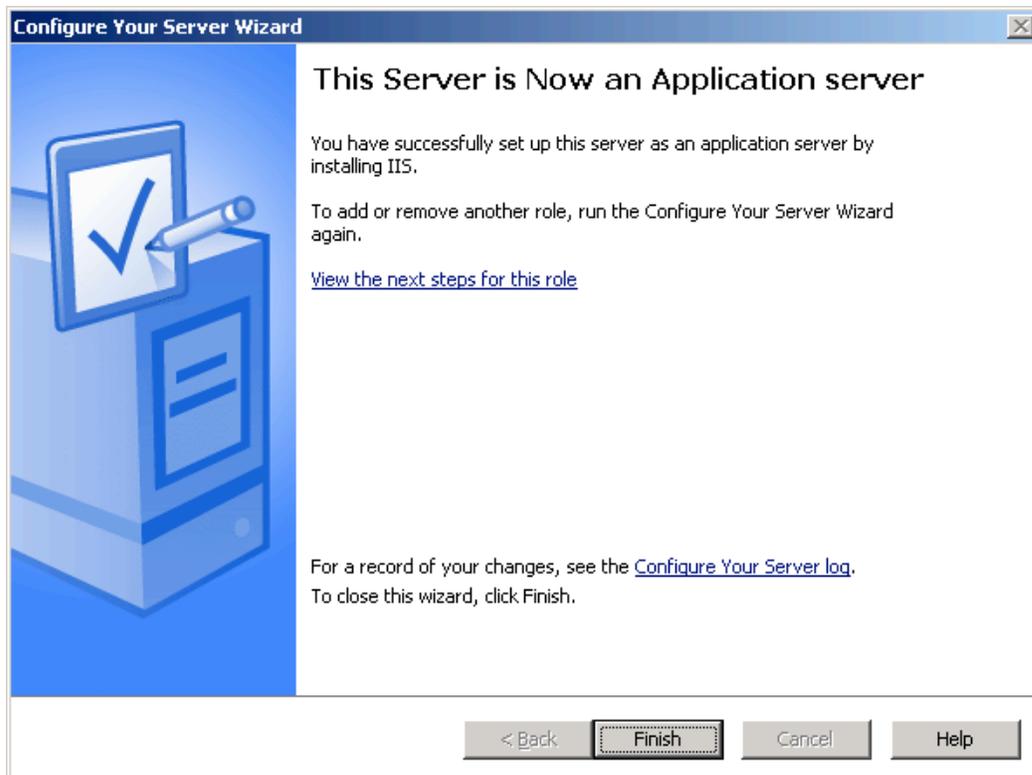
IIS will now be installed.



The wizard will change as IIS continues to be installed.

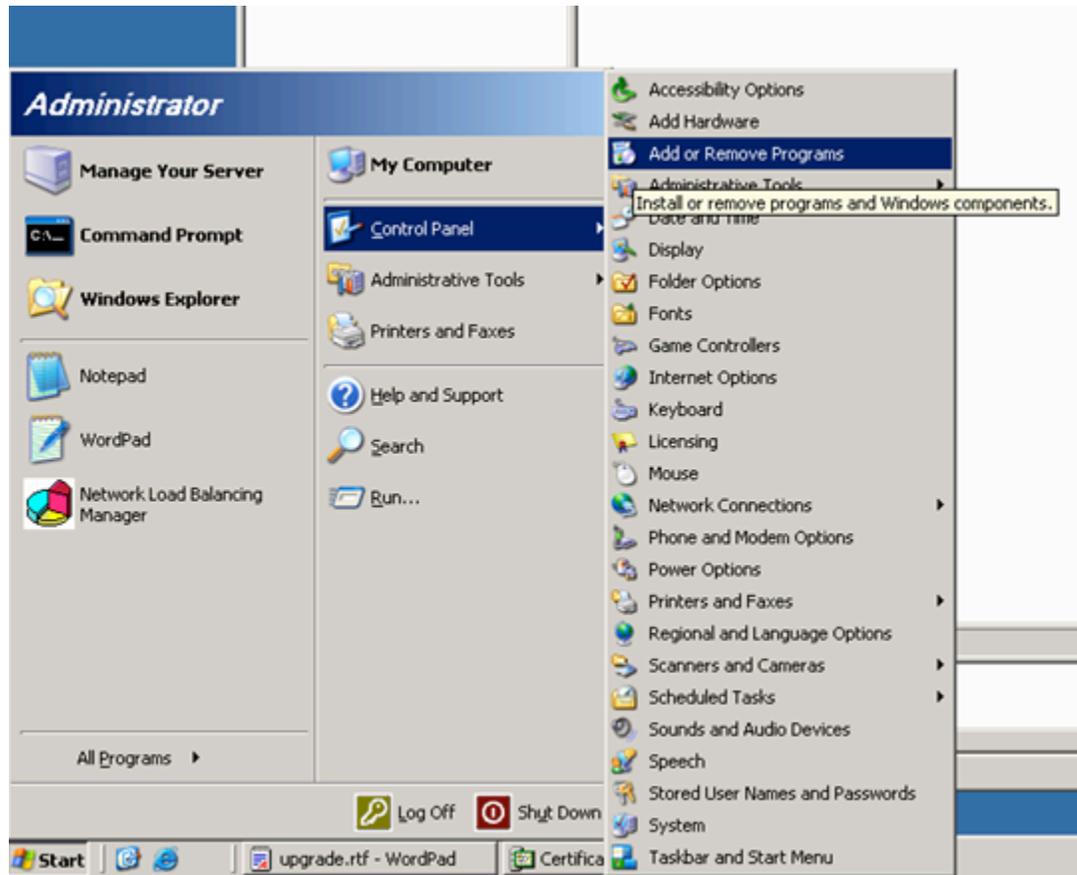


When IIS is finished installing you will see the window below.

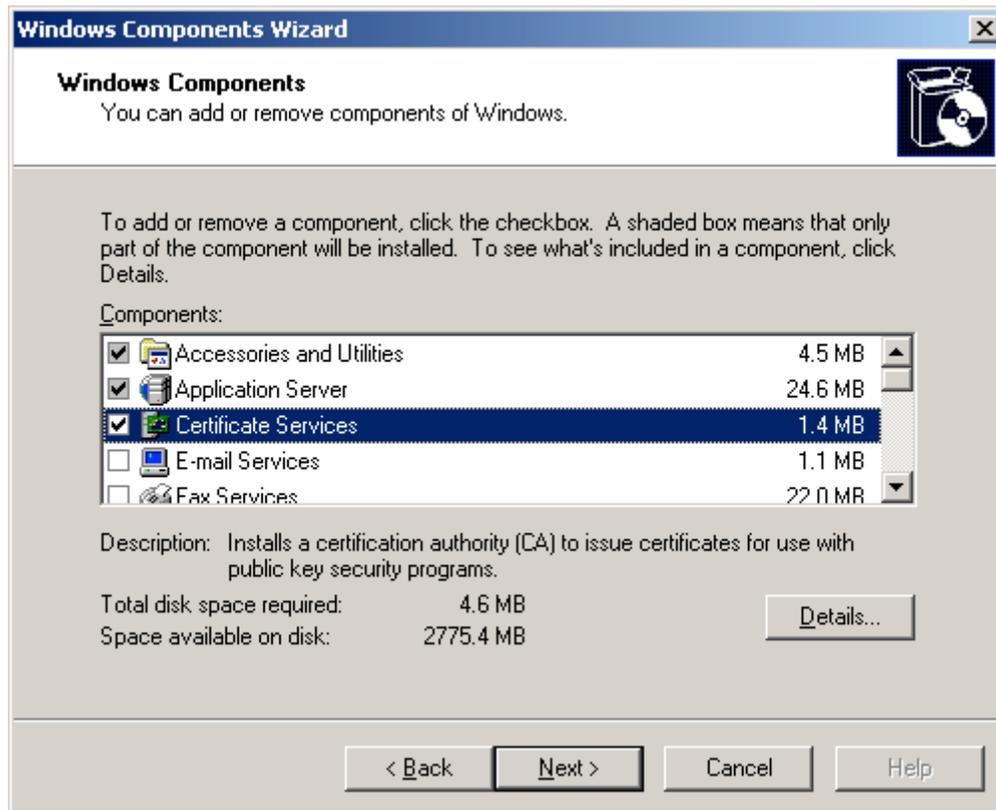


Configure the Server as a Certificate Authority

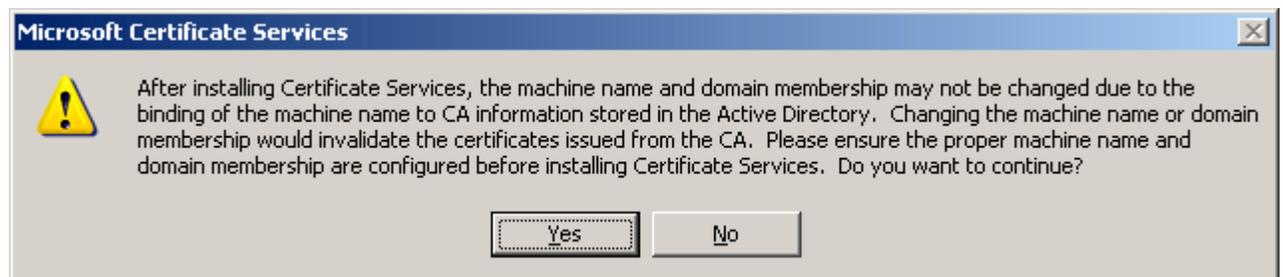
You can now configure the server to be a Certificate Authority. Start the process by selecting Start> Control Panel> Add or Remove Programs as shown below.



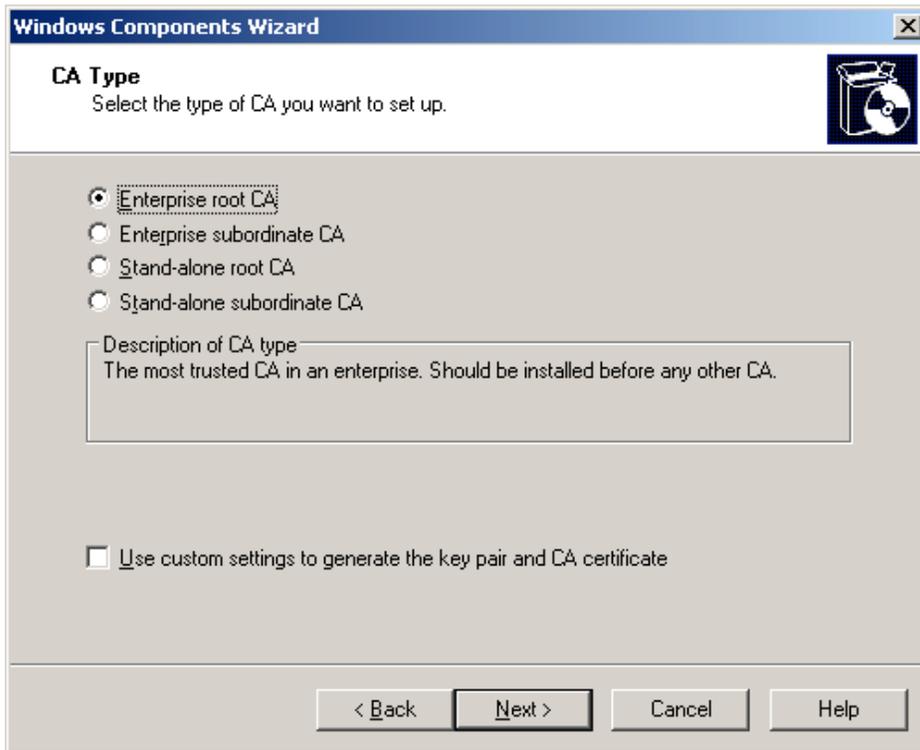
Select "Windows Components" and a list of windows components will be displayed. Now check the box next to "Certificate Services" and select "Next".



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

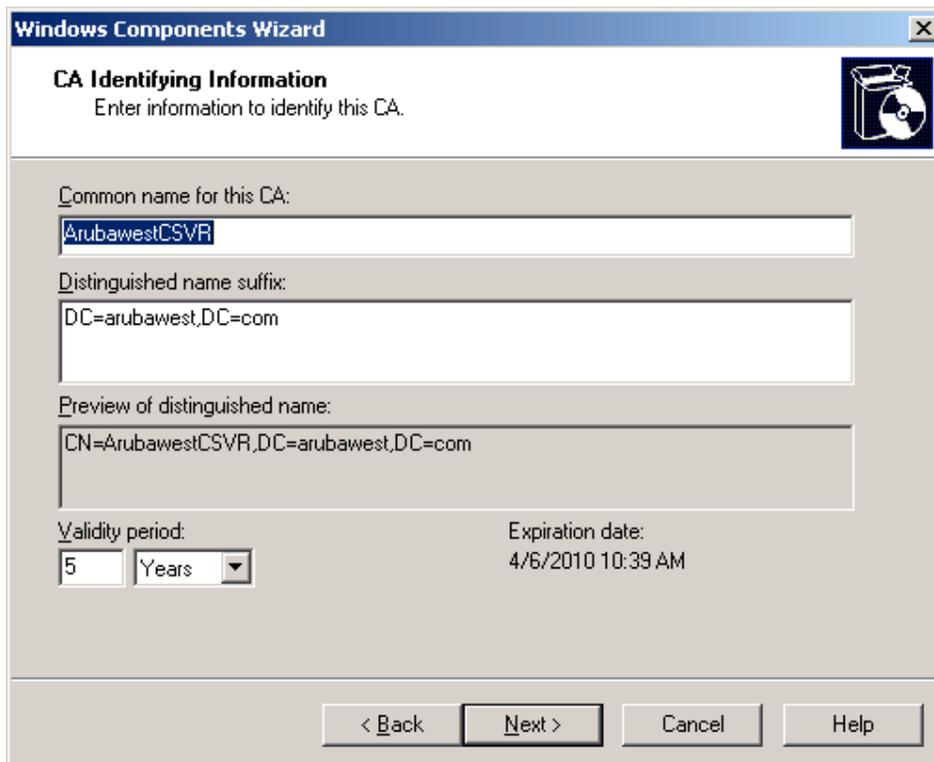


Now select the “Enterprise root CA” radio button, and select “Next” to continue.



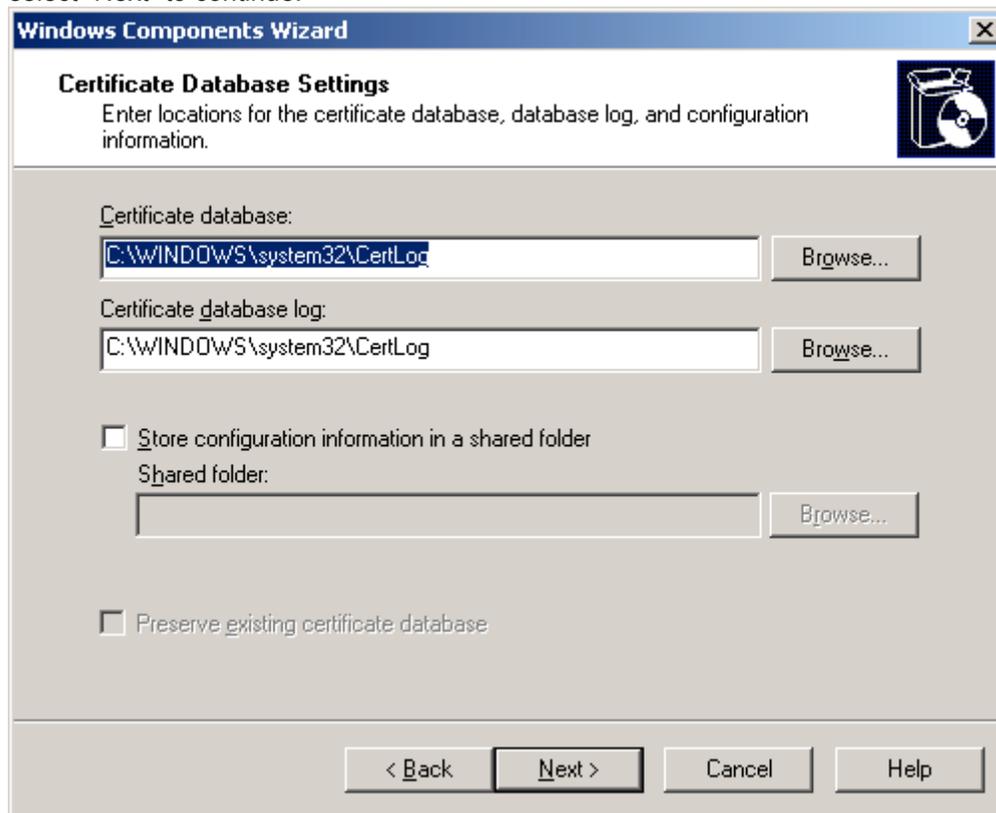
The screenshot shows the 'Windows Components Wizard' dialog box with the title 'CA Type'. The instruction reads 'Select the type of CA you want to set up.' There are four radio button options: 'Enterprise root CA' (selected), 'Enterprise subordinate CA', 'Stand-alone root CA', and 'Stand-alone subordinate CA'. Below these is a text box containing the description: 'Description of CA type: The most trusted CA in an enterprise. Should be installed before any other CA.' At the bottom, there is an unchecked checkbox labeled 'Use custom settings to generate the key pair and CA certificate'. 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' dialog box with the title 'CA Identifying Information'. The instruction reads 'Enter information to identify this CA.' It features 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, there is a 'Validity period' section with a text box containing '5' and a dropdown menu set to 'Years', and an 'Expiration date:' section with the value '4/6/2010 10:39 AM'. Navigation buttons at the bottom include '< Back', 'Next >', 'Cancel', and 'Help'.

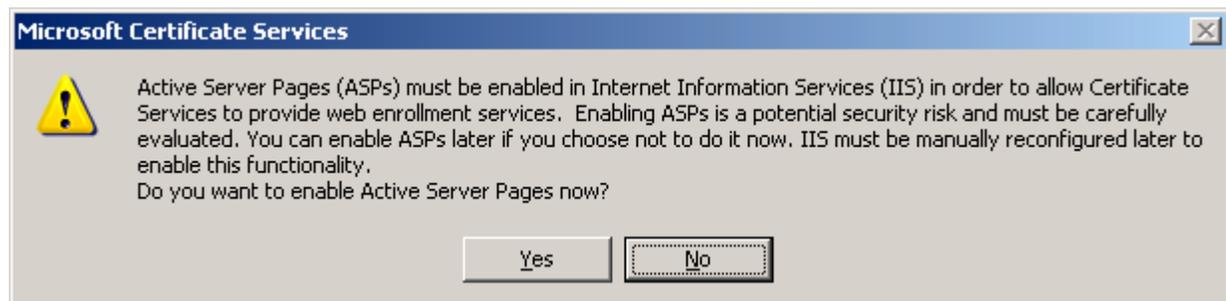
You will now be given an opportunity to change the location of the database and log files. Just select "Next" to continue.



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



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

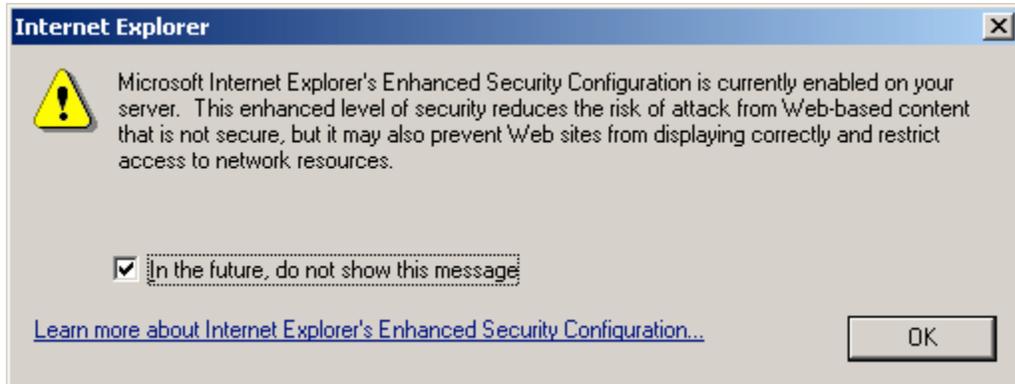


At this point the wizard is finished, and the server will now function as a CA.



Download the CA Certificate

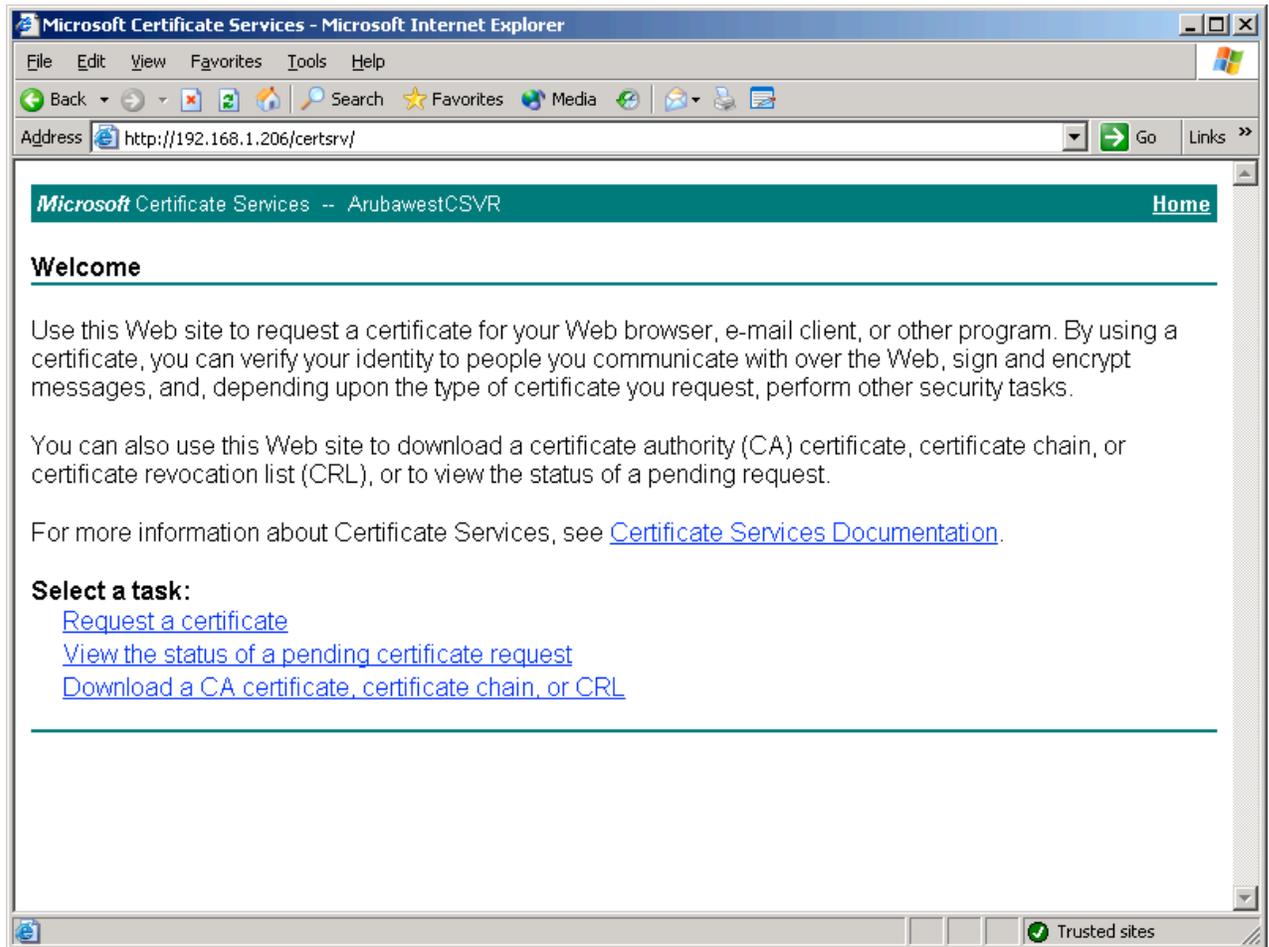
At this point you will need to Download the CA Certificate to make this server a trusted CA on this local machine. To do this you need to open a web browser and browse to the IP of this server and to the /certsrv page. In my case I needed to browse to <http://192.168.1.206/certsrv/>. Internet explorer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



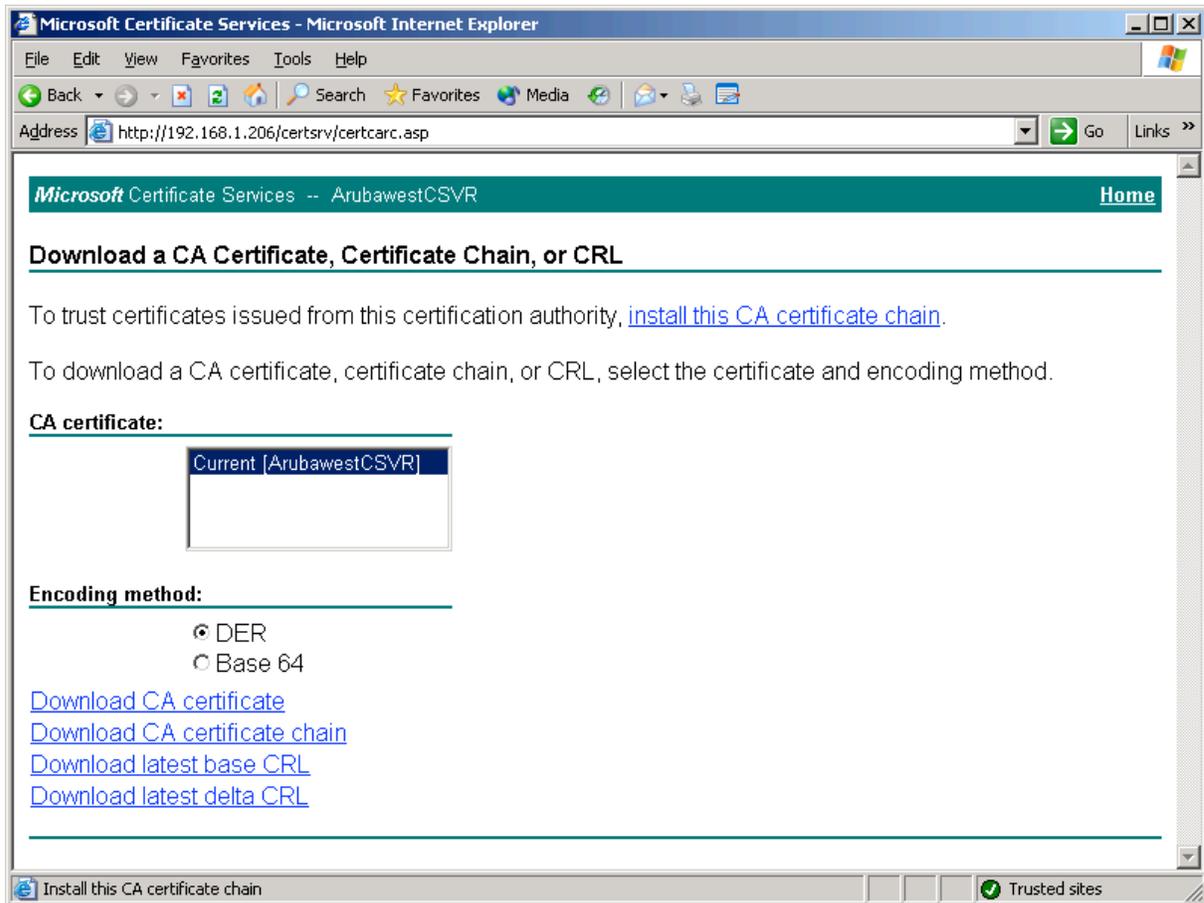
At this point you may be prompted with a login screen. You can use the administrator account and password.



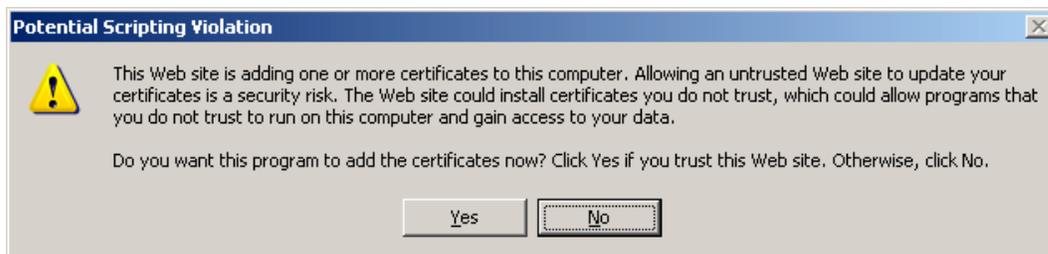
At this point you should see the web page as shown below. Select the link "Download a CA certificate, certificate chain, or CRL."



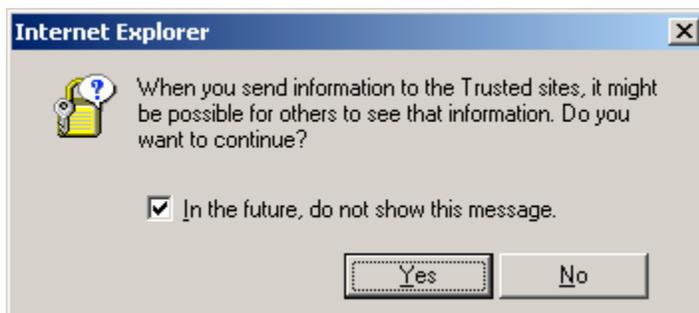
Now you will see the following page. Select the link “Install this CA certificate chain”.

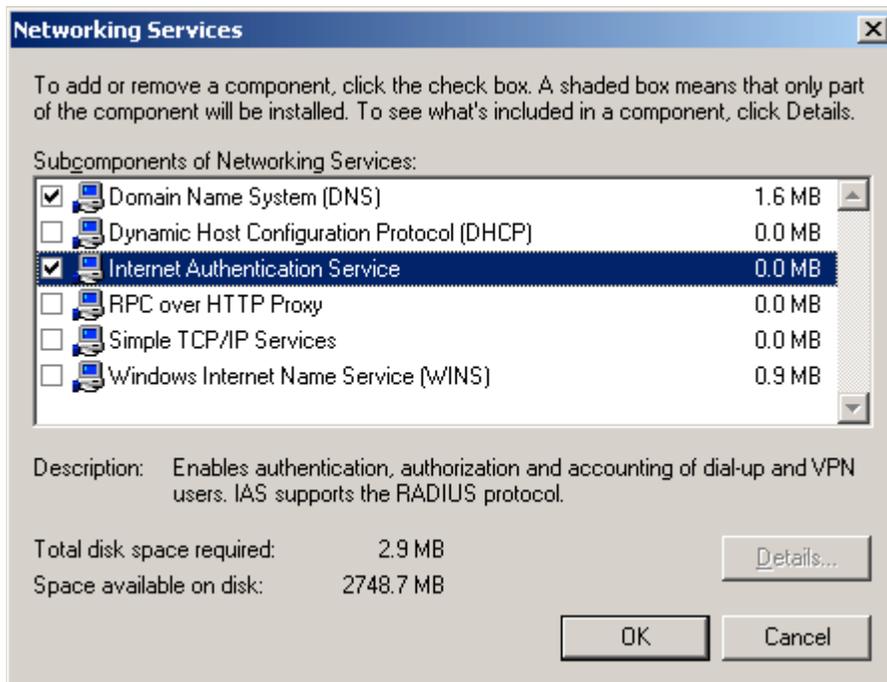
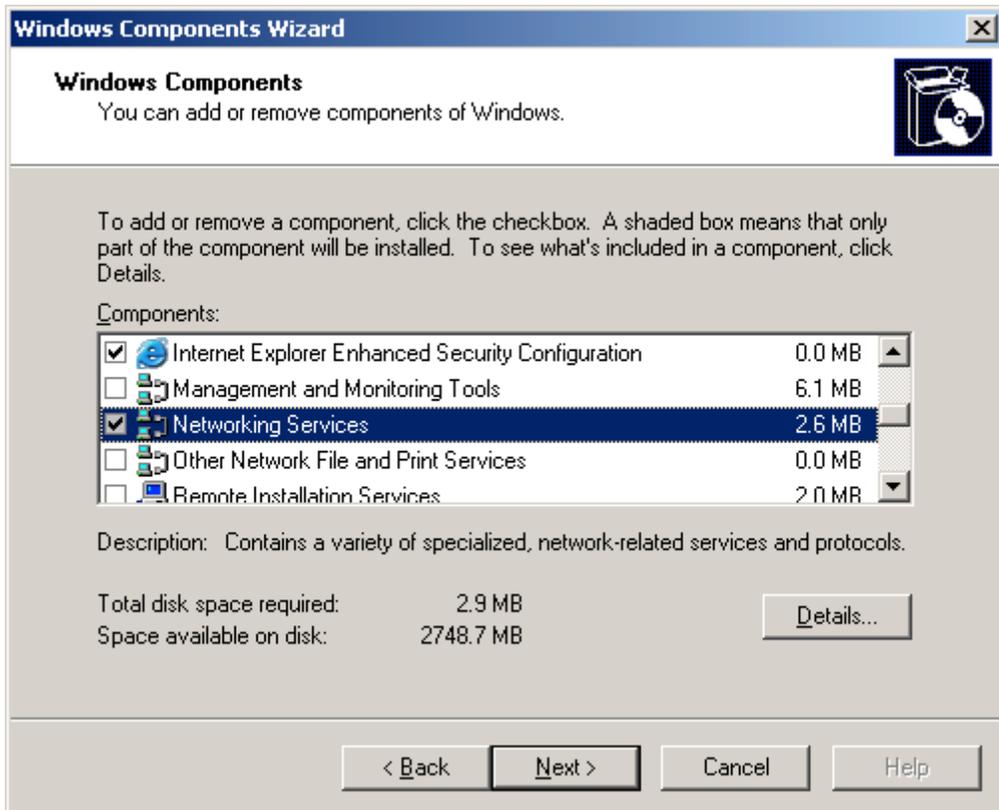


You will be prompted asking if you want to add the certificate. Select “Yes” to continue.



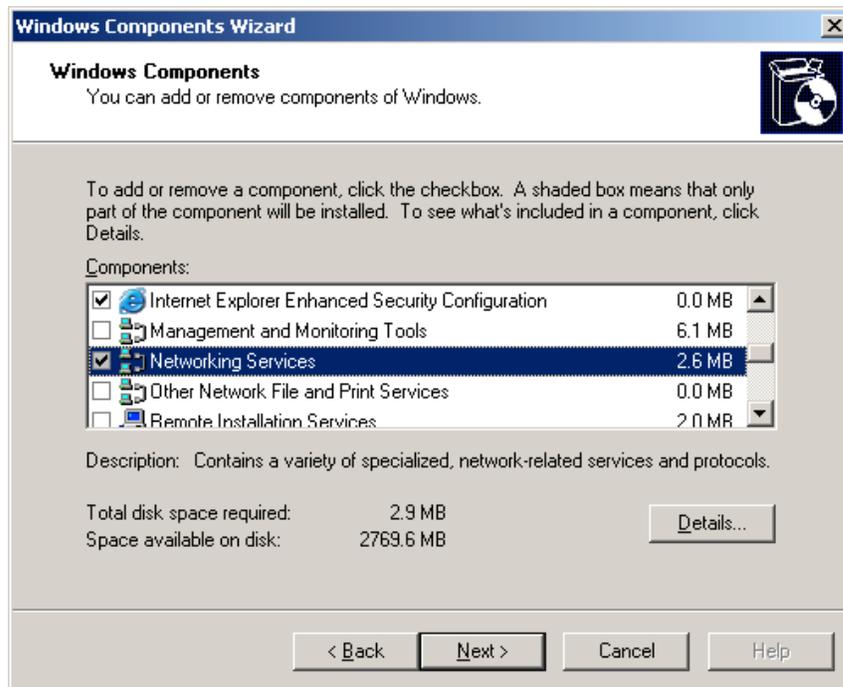
You may also see the following message. Select “Yes” to continue.





Enable and configure IAS

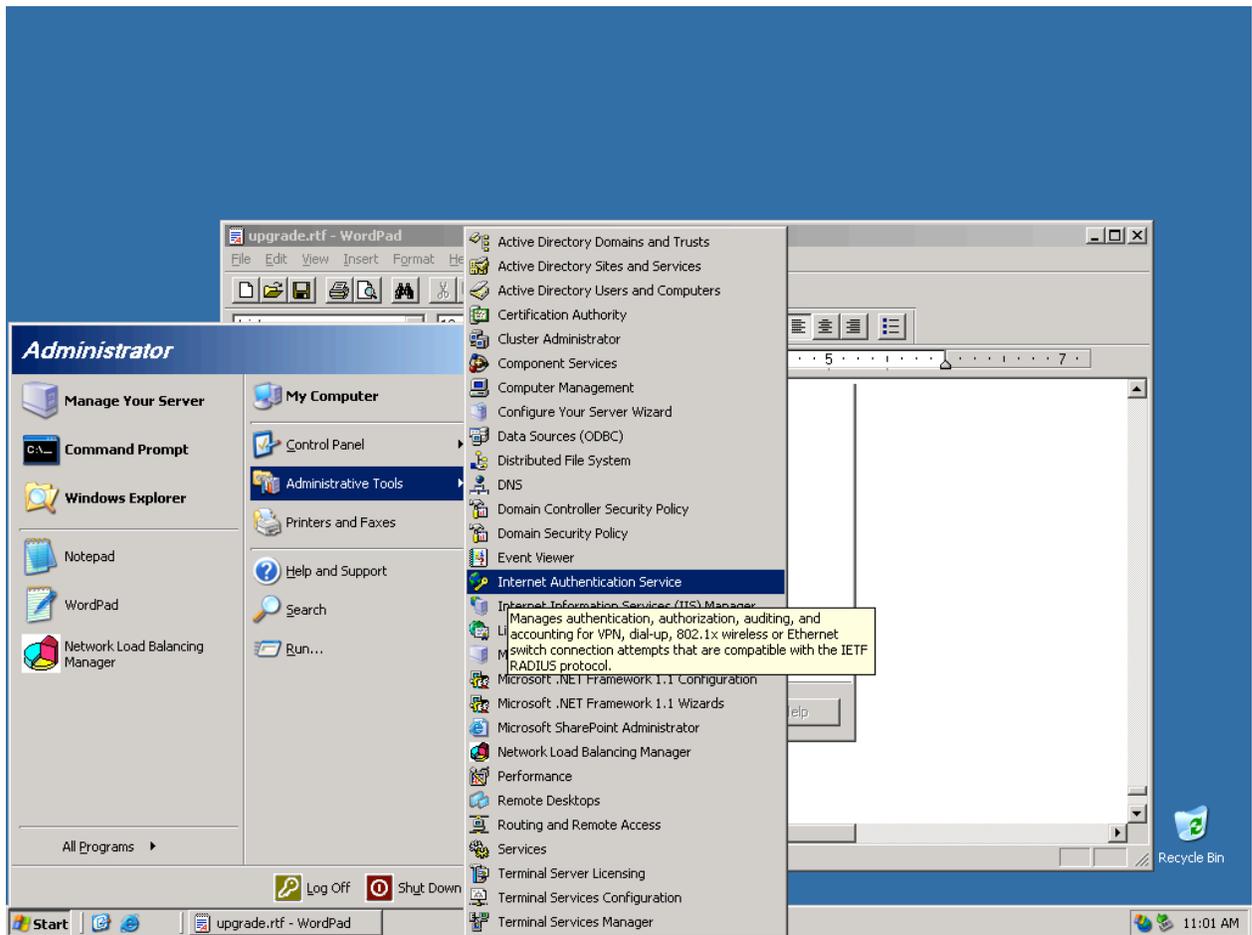
Now we are ready to install and configure IAS. Start the process by bring us the windows component wizard just as we did earlier for installing Certificate Services. Here you need to click on the “Networking Services” line to view all of the available services. Check the box next to “Internet Authentication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



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

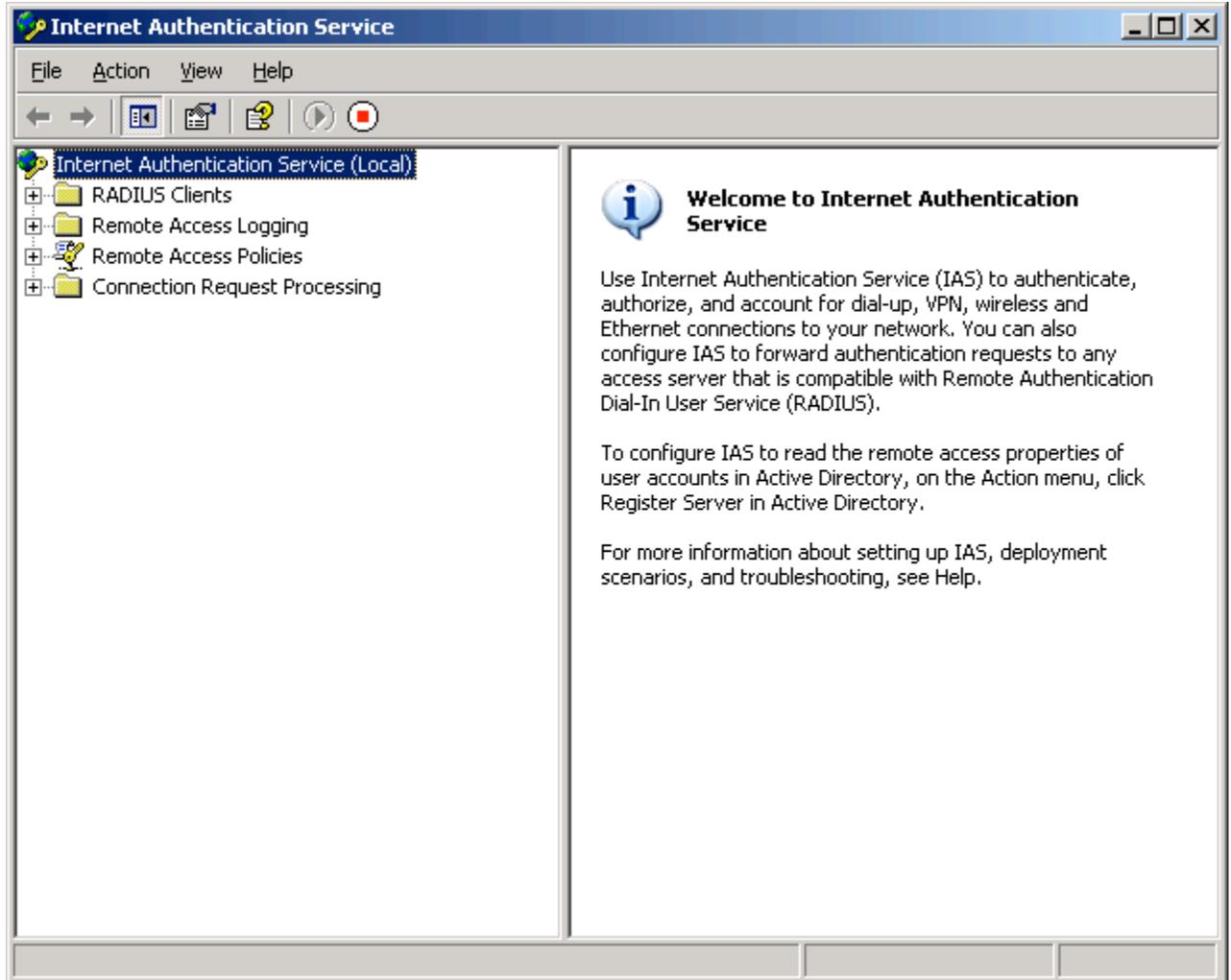


You can now configure IAS by going to Start>Administrative Tools>Internet Authentication Service> .

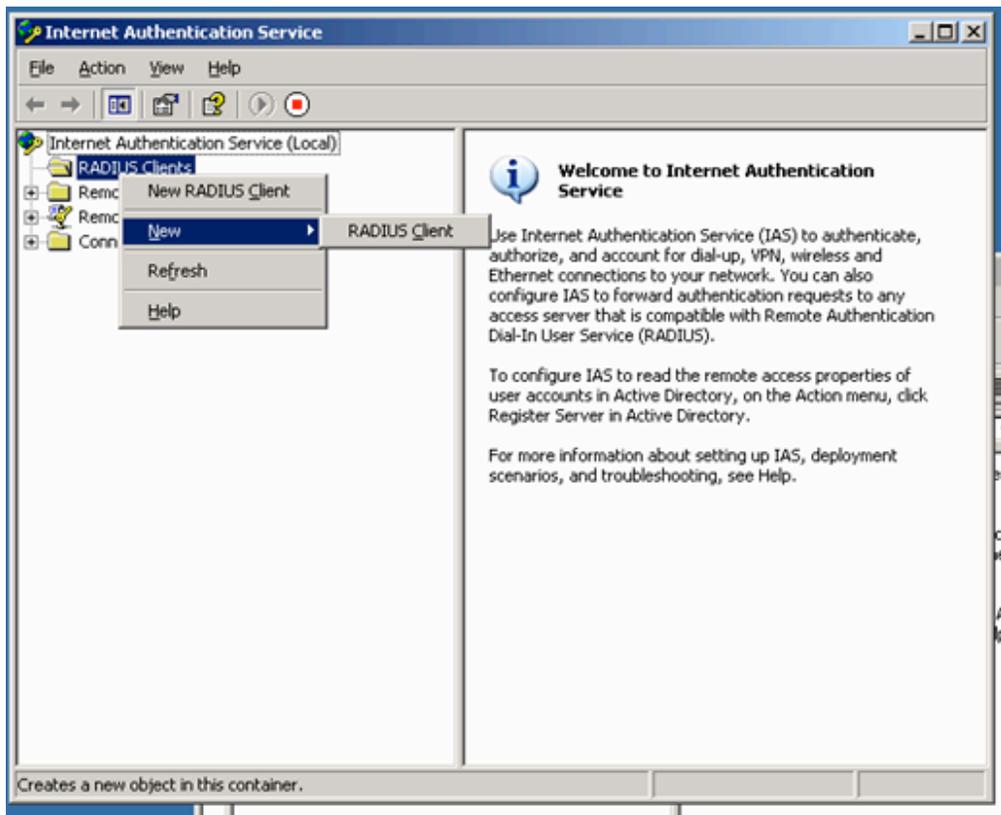


Here you will be presented with the IAS setup GUI.

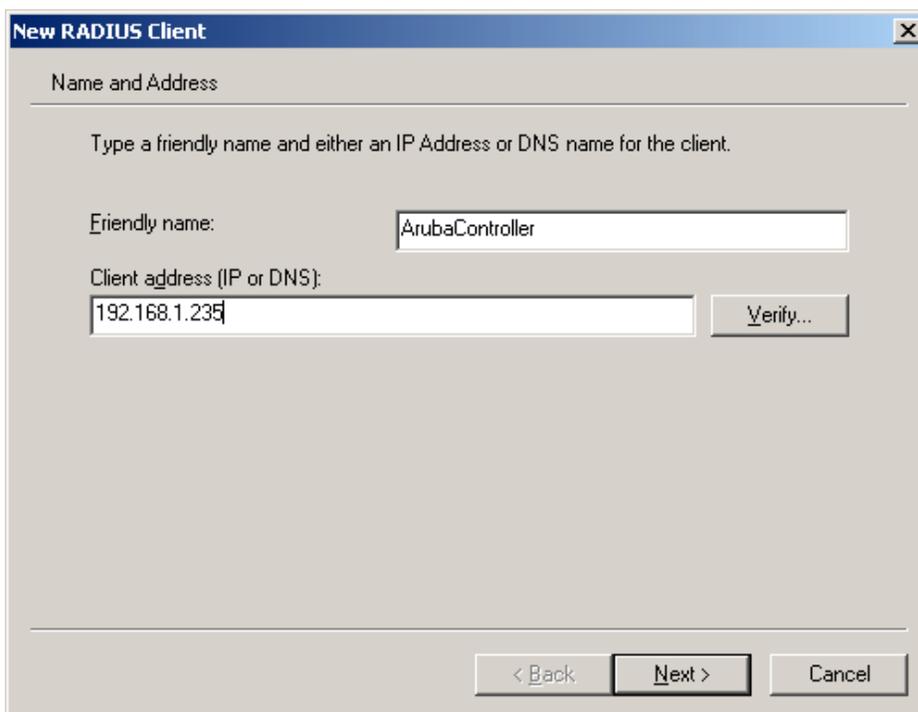
We will need to setup a Radius Client (The Aruba Controller) and a Remote Access Policy to be applied when users are authenticating.



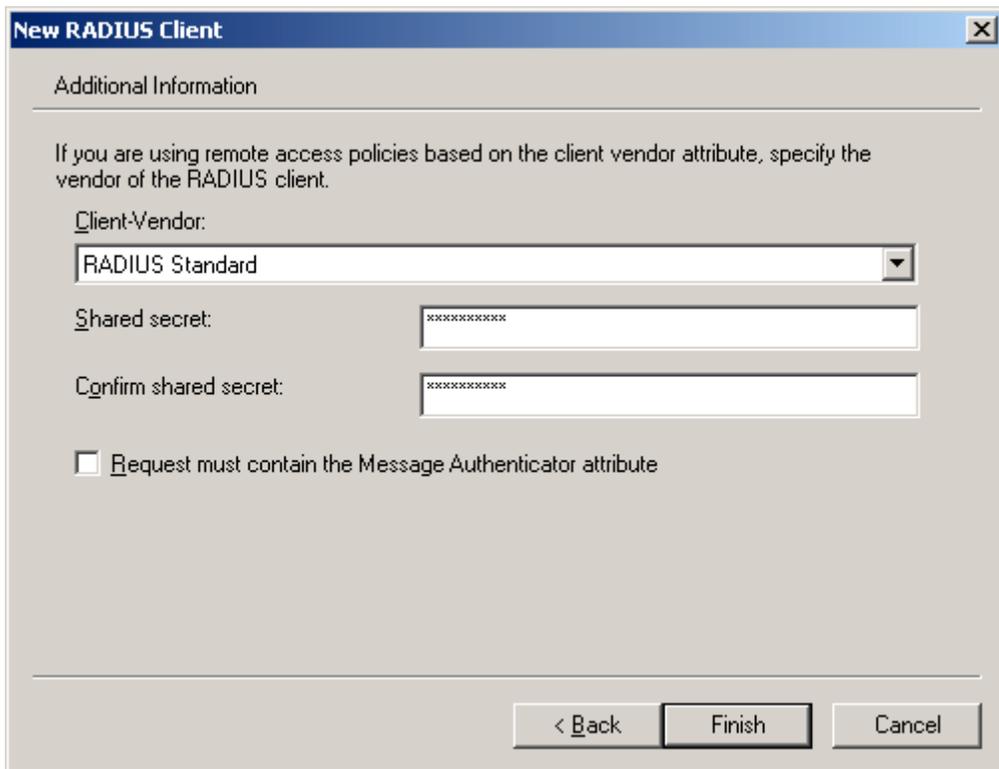
To add a radius client right click on the "Radius Client" folder and select New>Radius client.



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". The dialog has a blue title bar with a close button (X) in the top right corner. Below the title bar, the text "Additional Information" is displayed. A paragraph of text reads: "If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client." Below this text, there are three input fields: a dropdown menu for "Client-Vendor" with "RADIUS Standard" selected, a text box for "Shared secret" containing "*****", and another text box for "Confirm shared secret" also containing "*****". At the bottom left, there is a checkbox labeled "Request must contain the Message Authenticator attribute" which is currently unchecked. At the bottom right, there are three buttons: "< Back", "Finish", and "Cancel".

New RADIUS Client

Additional Information

If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.

Client-Vendor: RADIUS Standard

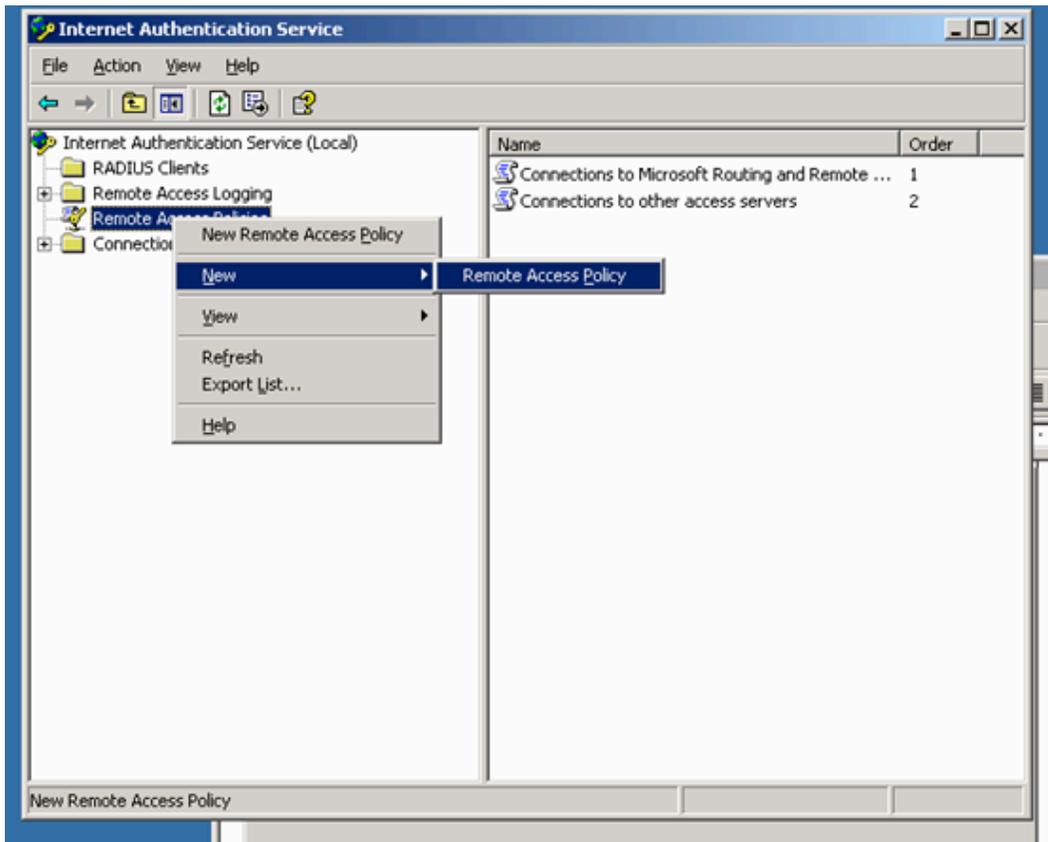
Shared secret: *****

Confirm shared secret: *****

Request must contain the Message Authenticator attribute

< Back Finish Cancel

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.



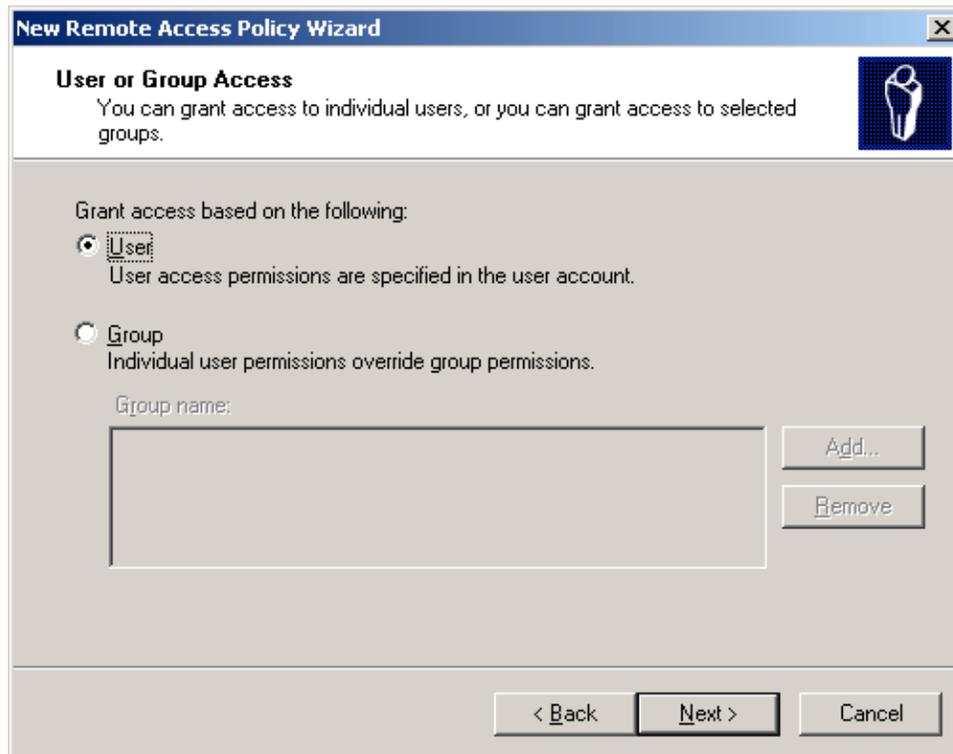
First you need to give the policy a name, and select “Next” to continue

The screenshot shows a dialog box titled "New Remote Access Policy Wizard" with a close button in the top right corner. The main heading is "Policy Configuration Method" and the subtext reads "The wizard can create a typical policy, or you can create a custom policy." Below this, the question "How do you want to set up this policy?" is 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". A text prompt asks the user to "Type a name that describes this policy." Below this is a text input field containing "Aruba Users" and an example text "Example: Authenticate all VPN connections." At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

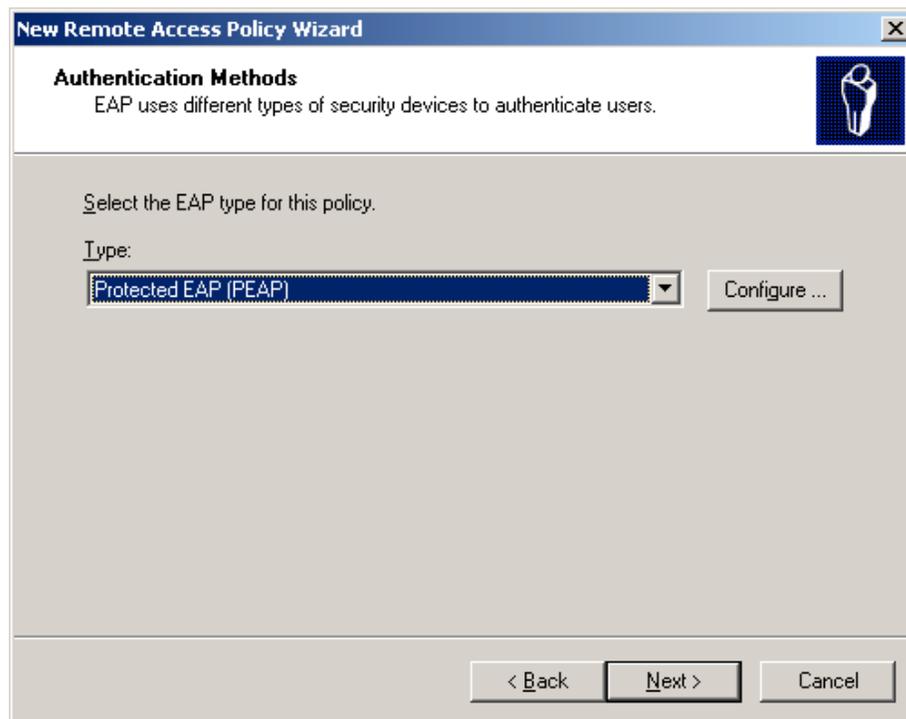
Next select “Wireless” as the access method, and select “Next” to continue.

The screenshot shows the same dialog box, now at the "Access Method" step. The subtext reads "Policy conditions are based on the method used to gain access to the network." Below this, the instruction "Select the method of access for which you want to create a policy." is followed by four radio button options: "VPN" (with subtext "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 subtext "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 dashed border around the text, with subtext "Use for wireless LAN connections only."), and "Ethernet" (with subtext "Use for Ethernet connections, such as connections that use a switch."). At the bottom are the same three buttons: "< Back", "Next >", and "Cancel".

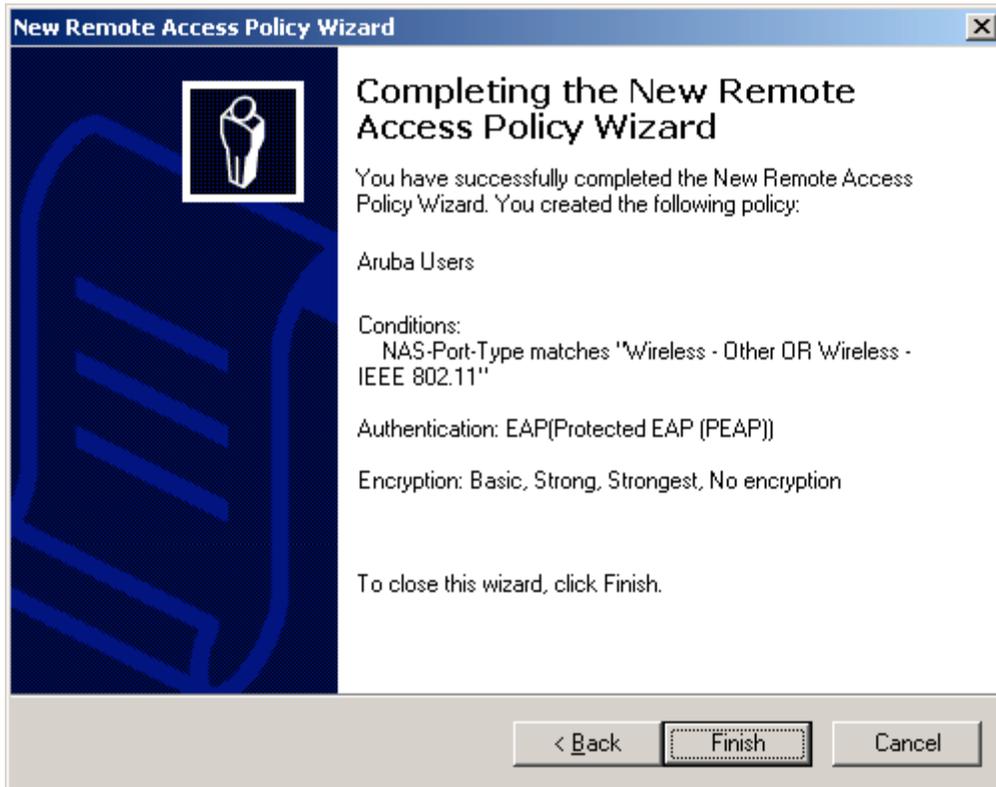
Now you will be asked if you want to grant access by individual user or by groups. In the example below, User is chosen. Select "Next" to continue.



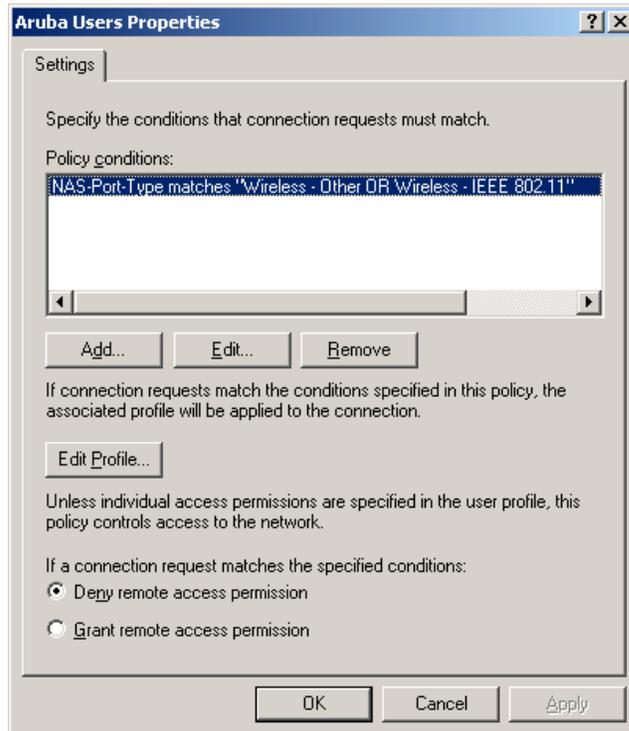
Now you will be asked what EAP type to use. IAS only supports PEAP and EAP-TLS. In this example PEAP is selected. Select "Next" to continue.

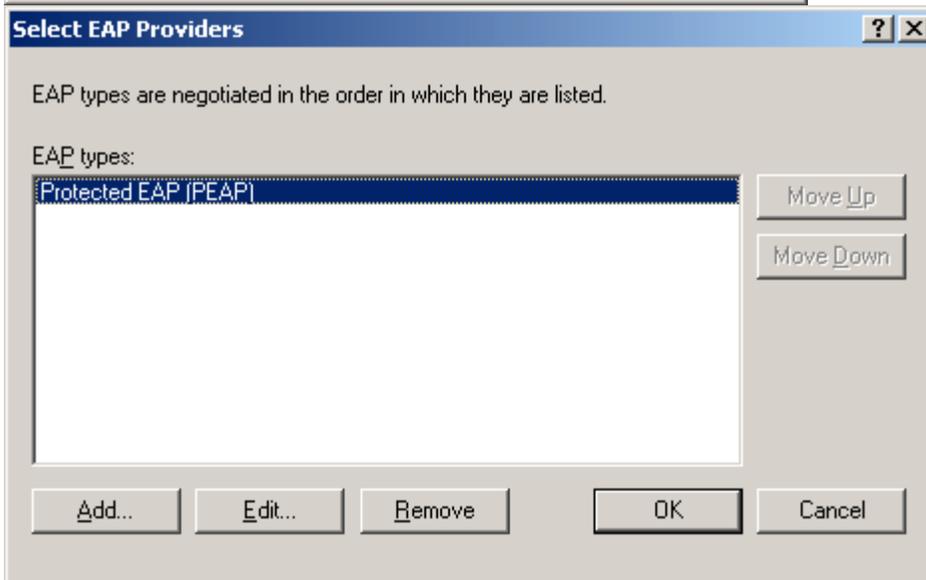
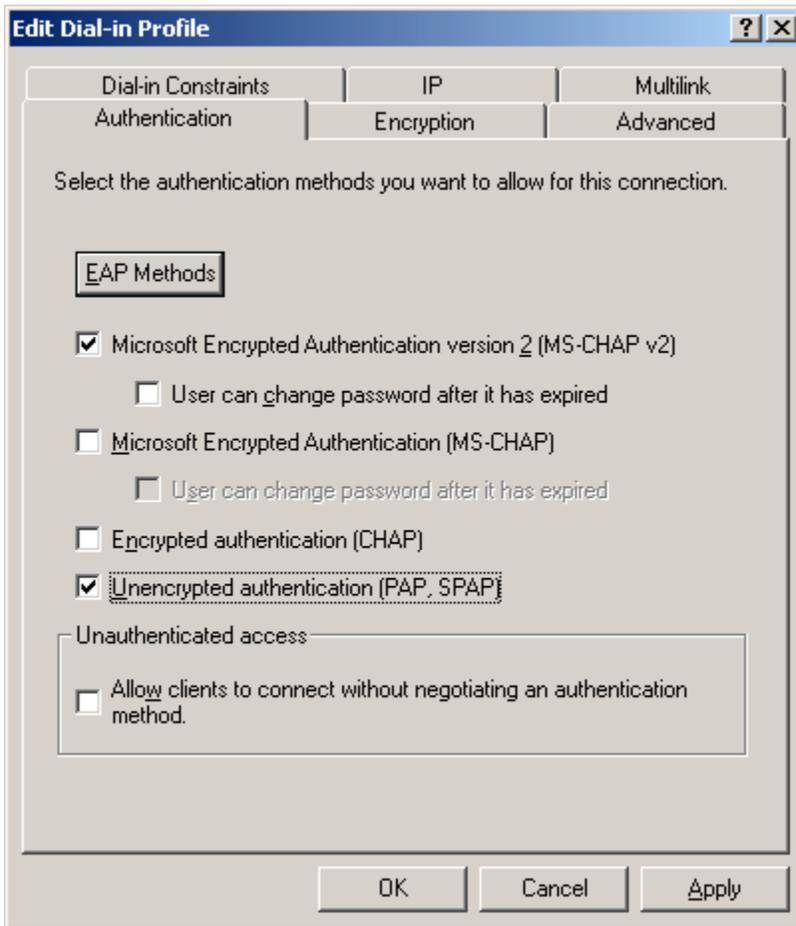


The following window will be displayed. Select "Finish".



The new policy will be added





Dial-in Settings



You selected one or more authentication methods. To ensure that each protocol is correctly configured for the remote access, policy, and domain levels, follow the step-by-step procedures in Help.

View the corresponding Help topic?

Yes

No

Internet Authentication Service

File Action View Help

Internet Authentication Service (Local)

- RADIUS Clients
- Remote Access Logging
- Remote Access Policies
- Connection Request Processing

Name	O...	▲
Aruba Users	1	
Connections to Microsoft Routing and Remote ...	2	
Connections to other access servers	3	

Administrator

Manage Your Server

- Command Prompt
- Windows Explorer
- Notepad
- WordPad
- Network Load Balancing Manager

All Programs ▶

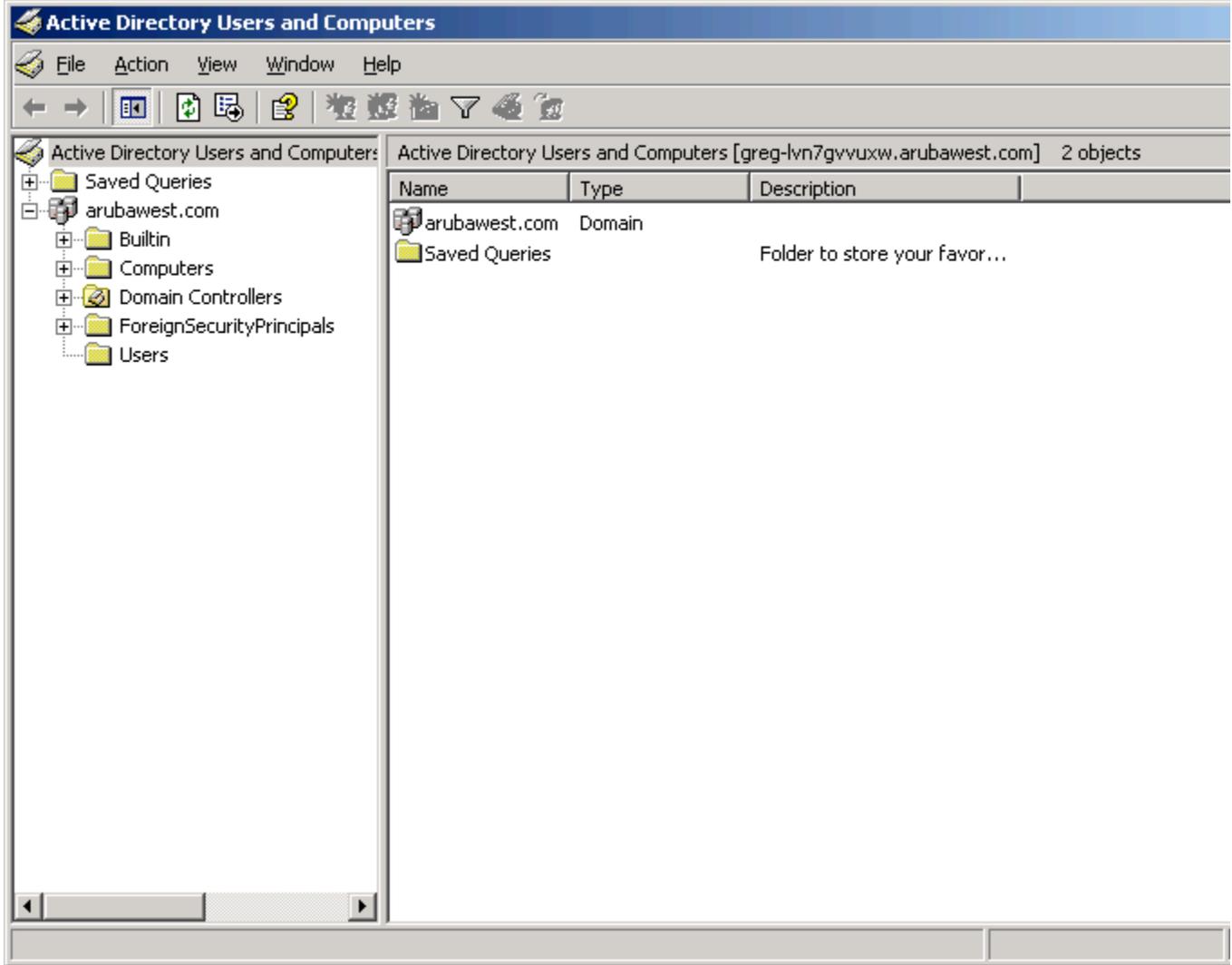
My Computer

- Control Panel
- Administrative Tools
- Printers and Faxes
- Help and Support
- Search
- Run...

- Active Directory Domains and Trusts
- Active Directory Sites and Services
- Active Directory Users and Computers**
- Certification Authority
- Manages users, computers, security groups and other objects in the Active Directory.
- Component Services
- Computer Management
- Configure Your Server Wizard
- Data Sources (ODBC)
- Distributed File System
- DNS
- Domain Controller Security Policy
- Domain Security Policy
- Event Viewer
- Internet Authentication Service
- Internet Information Services (IIS) Manager
- Licensing
- Manage Your Server
- Microsoft .NET Framework 1.1 Configuration
- Microsoft .NET Framework 1.1 Wizards
- Microsoft SharePoint Administrator
- Network Load Balancing Manager
- Performance
- Remote Desktops
- Routing and Remote Access
- Services
- Terminal Server Licensing
- Terminal Services Configuration
- Terminal Services Manager

Log Off Shut Down

Start | upgrade.rtf - WordPad (...)



Active Directory Users and Computers

File Action View Window Help

Active Directory Users and Computers: Users 21 objects

Name	Type	Description
Administrator	User	Built-in account for admini...
Cert Publishers	Security Group ...	Members of this group are...
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdatePr...	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Comp...	Security Group ...	All workstations and serve...
Domain Contr...	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Ad...	Security Group ...	Designated administrators...
Group Policy ...	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
HelpServices...	Security Group ...	Group for the Help and Su...
IIS_WPG	Security Group ...	IIS Worker Process Group
IUSR_GREG-L...	User	Built-in account for anyony...
IWAM_GREG-...	User	Built-in account for Intern...
OWS_171398...	Security Group ...	Microsoft SharePoint role '...
RAS and IAS ...	Security Group ...	Servers in this group can ...
Schema Admins	Security Group ...	Designated administrators...
SUPPORT_38...	User	This is a vendor's account ...
TelnetClients	Security Group ...	Members of this group ha...

New Object - User X

 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

New Object - User X

 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.

Active Directory Users and Computers

File Action View Window Help

Active Directory Users and Computers: Users 22 objects

Name	Type	Description
Administrator	User	Built-in account for admini...
Cert Publishers	Security Group ...	Members of this group are...
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdatePr...	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Comp...	Security Group ...	All workstations and serve...
Domain Contr...	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Ad...	Security Group ...	Designated administrators...
Greg Pifer	User	
Group Policy ...	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
HelpServices...	Security Group ...	Group for the Help and Su...
IIS_WPG	Security Group ...	IIS Worker Process Group
IUSR_GREG-L...	User	Built-in account for anyony...
IWAM_GREG-...	User	Built-in account for Intern...
OWS_171398...	Security Group ...	Microsoft SharePoint role '...
RAS and IAS ...	Security Group ...	Servers in this group can ...
Schema Admins	Security Group ...	Designated administrators...
SUPPORT_38...	User	This is a vendor's account ...
TelnetClients	Security Group ...	Members of this group ha...

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