

## Installing a Domain Controller

This is the second document in a series of 3. First use the document Lab Setup, then this Domain Controller document, and finally the WEP Enterprise document.

In order to setup Windows based RADIUS, the following steps have to be done:

1. Install a Domain Controller and DNS
2. Install IIS and CA as the Enterprise Root CA
3. Install IAS and setup user accounts.

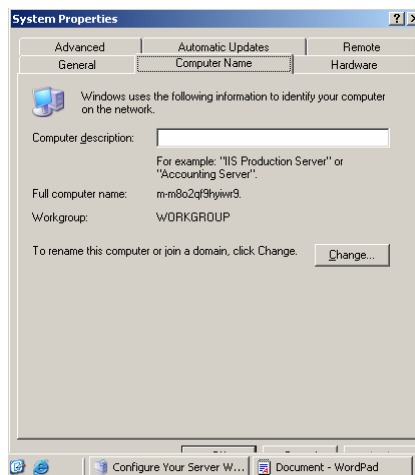
Each of these steps will be broken down in finer detail. The system will be configured to use WPA Enterprise V1 + AES

### 1. Install a Domain Controller and DNS.

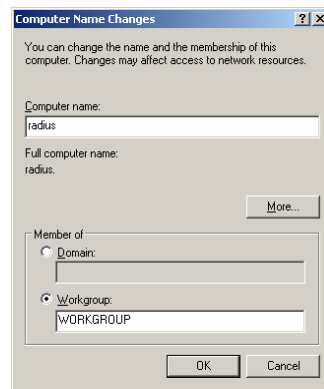
#### 1.1. Setup the NetBIOS name

To avoid any assumptions, we begin with setting the Computer Name (NetBIOS).

1. Right click on **My Computer**
2. Choose **Properties**,
3. On **System Properties**, click on the **Computer Name** tab. (See below figure)



4. Click Change

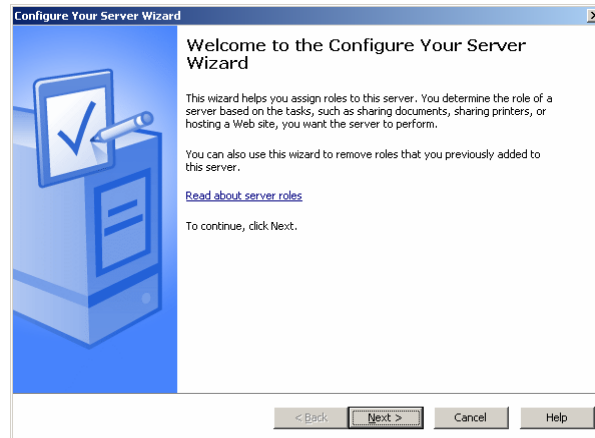


5. Type in the NetBIOS name (this will become part of the fully qualified domain name)
6. Click OK, then OK, then OK, then Yes and allow for a restart.

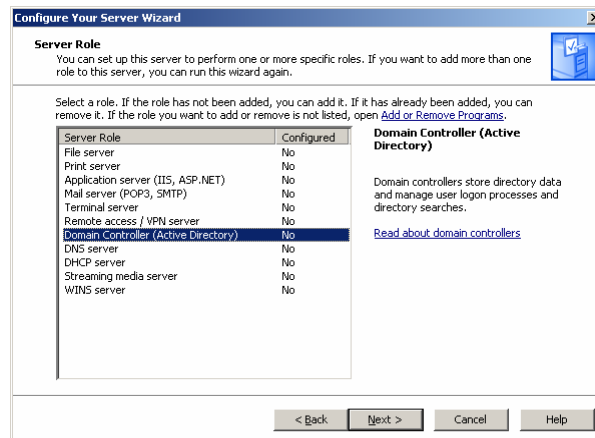
## 1.2. Installing a Domain Controller.

1. Click the Start Button
2. Click Programs
3. Click Administrative Tools
4. Click Configure Your Server Wizard

The Configure Your Server Wizard displays.

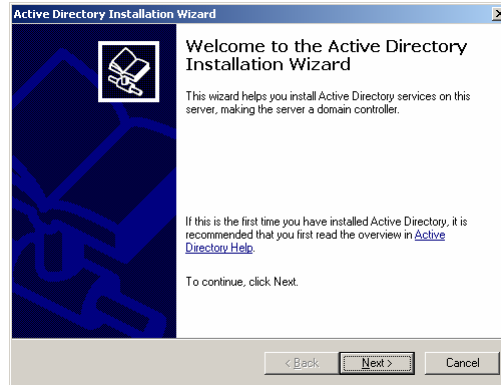


5. Click the Next button

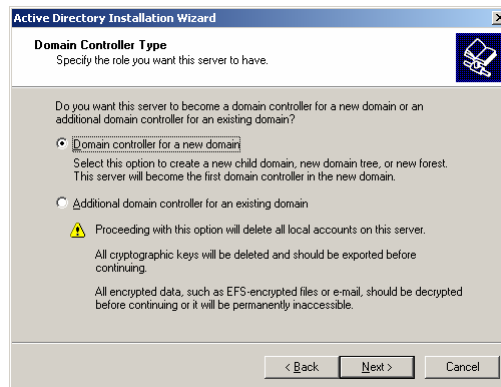


6. Choose Domain Controller
7. Click Next, then Next

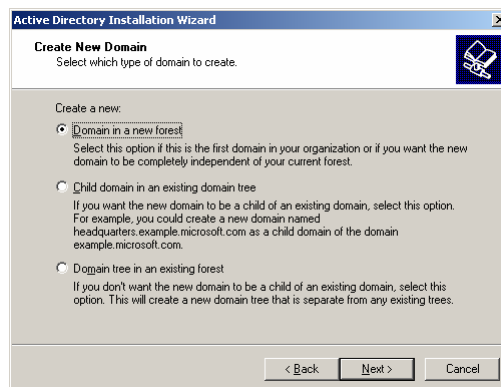
The Active Directory Installation Wizard displays.



8. Click Next  
The Domain Controller Type window displays.

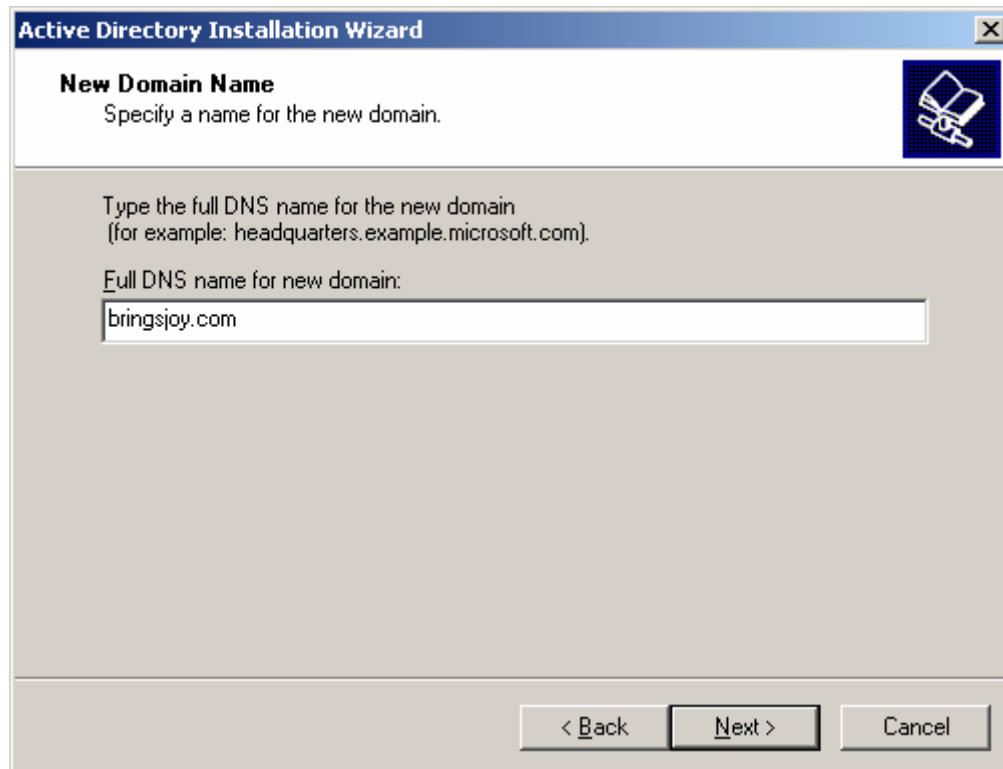


9. Click Next  
The Create New Domain window displays.



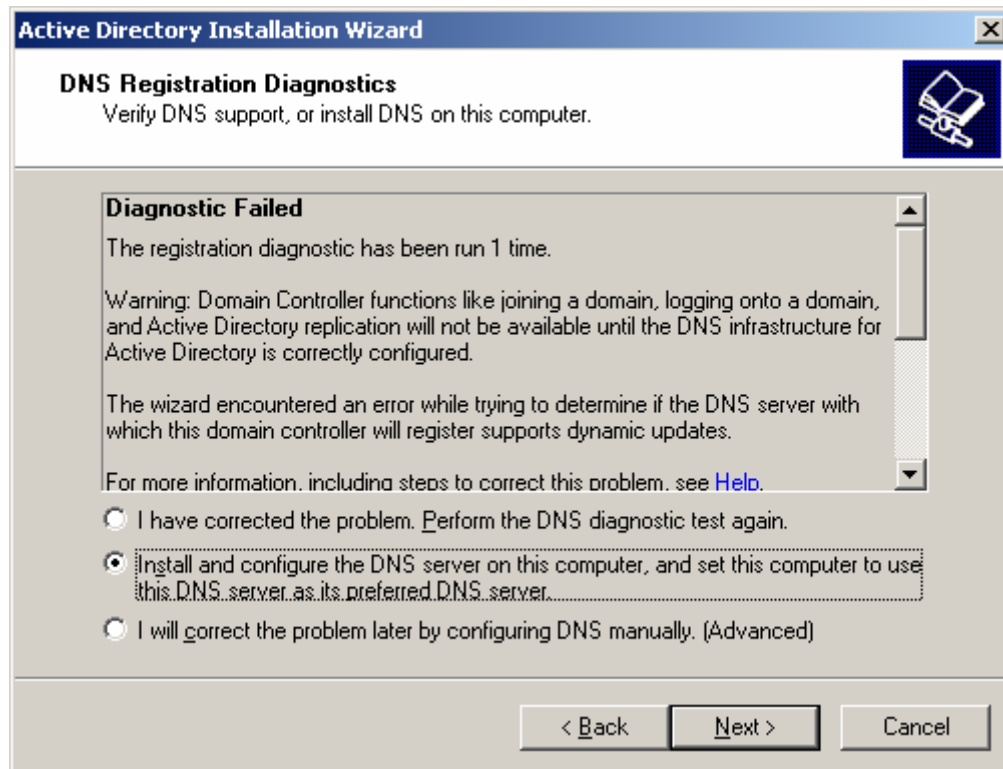
10. Click Next

The New Domain Name window displays.



11. Enter the domain name as shown above (bringsjoy.com)
12. Click Next, then Next, then Next, then Next

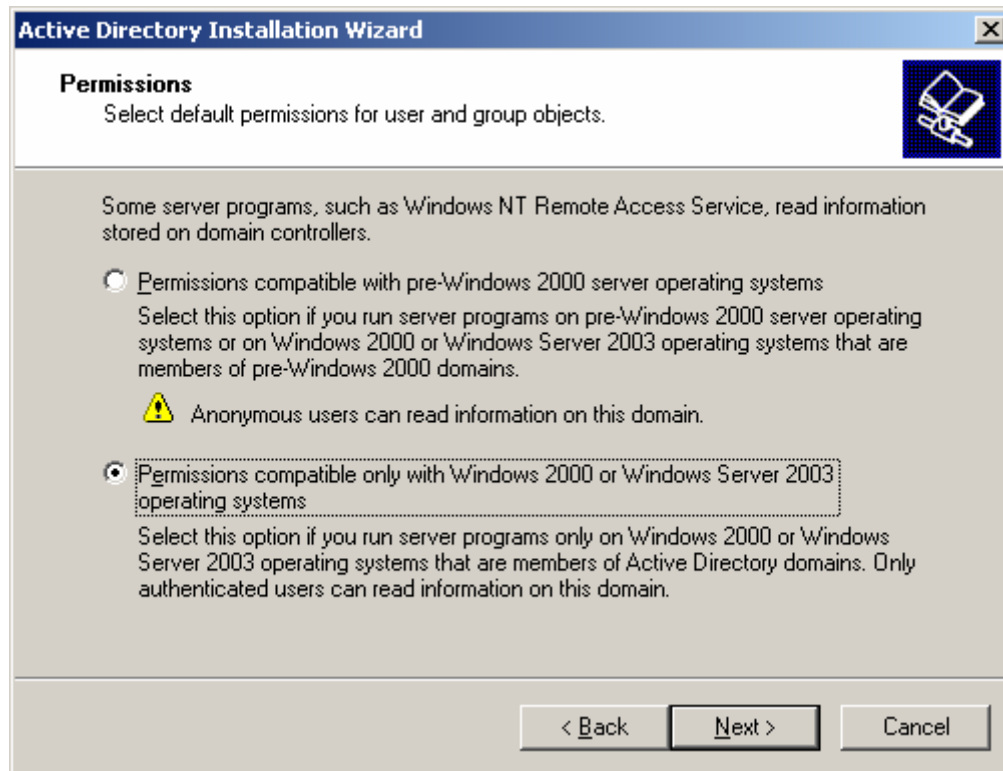
The DNS Registration Diagnostics window displays.



13. Choose the second radio button

14. Click Next

The Permissions window displays.



15. Choose the second radio button and click Next.

16. Either enter PASSWORDx2, or leave it blank

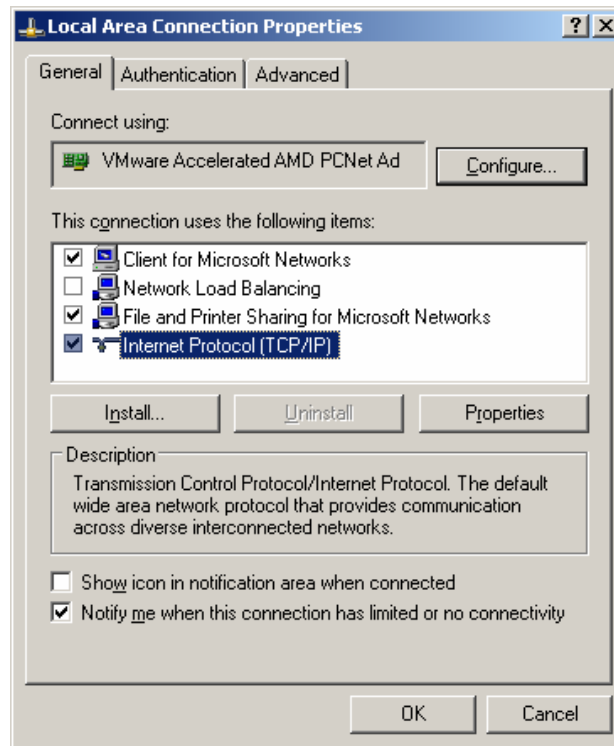
17. Click Next, then Next, and wait 4 hours.

1.3. DNS Setup follows.



1. Click Ok

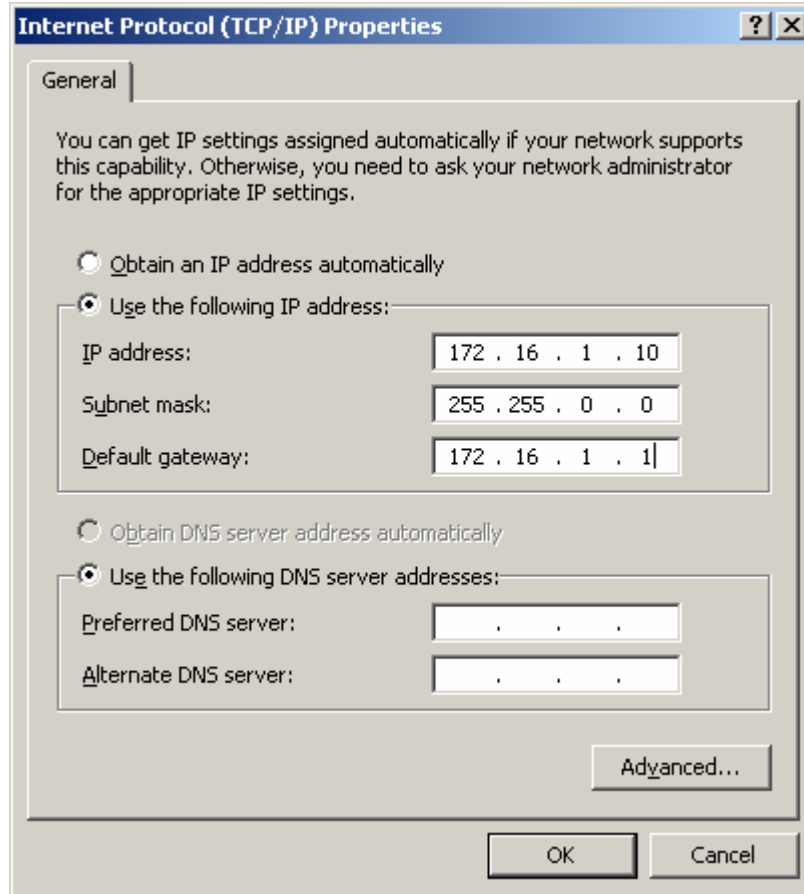
The Local Area Connection Properties window displays.



2. Choose Internet Protocol (TCP/IP)
3. Place a check mark on [Show icon in...]
4. Click on the Properties button



The Local Area Connection Properties window displays.



5. Fill the information as shown above [
  - IP address:172.16.1.10/16
  - Subnet mask 255.255.0.0
  - Default Gateway: 172.16.1.1
6. Click OK and OK  
Remember that we are setting up also a DNS server
7. Click the Close button
  - DNS registration will start as part of the DC setup
  - DO NOT CLICK on skip DNS installation
8. Choose Finish, then Restart Now
9. Once restarted click on the Finish button.

## 2. CA and IIS

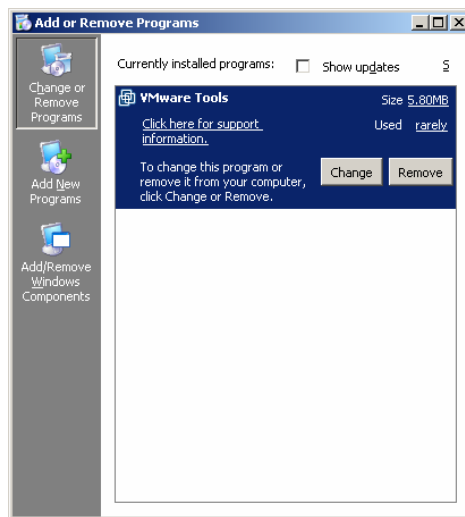
Although it is possible to add the CA server and IIS services at the same time, the steps that follow will do it separately. I have noticed that when installed at the same time, a small popup error message comes up in regards to the CA.

### 2.1. Installing IIS

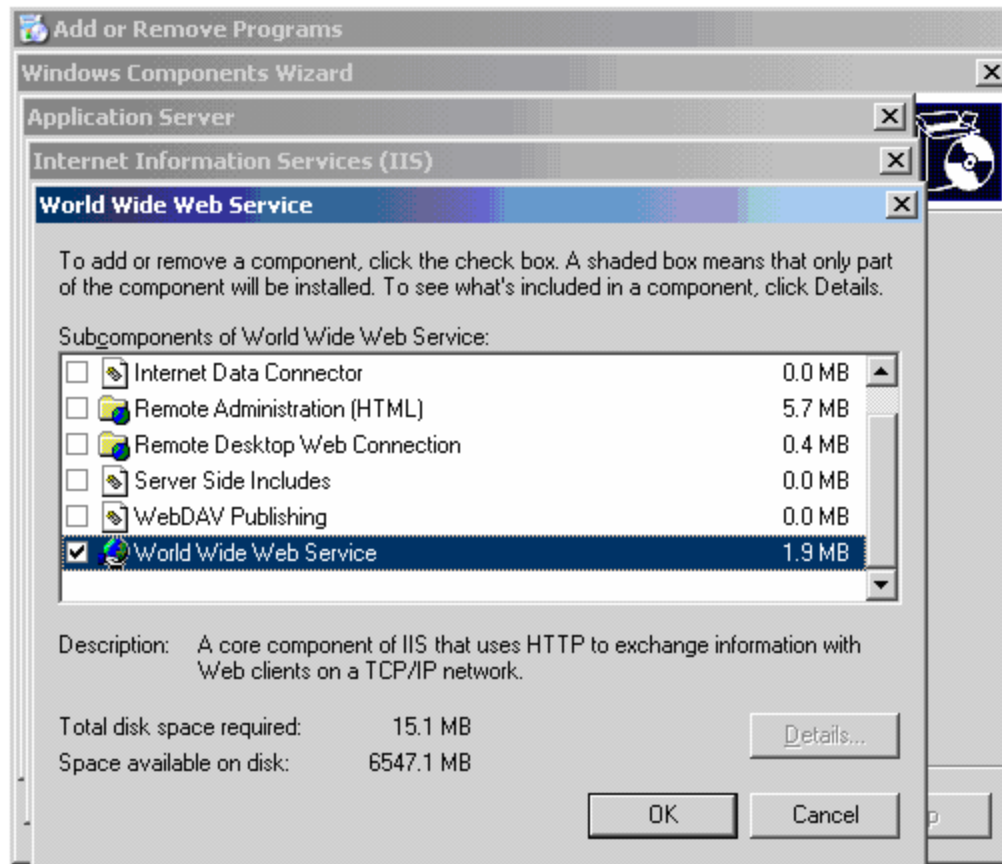
IIS is used as one channel to send a certificate to the wireless client.

1. Click the Start Button
2. Click Control Panel
3. Click Add or Remove Programs

The Local Area Connection Properties window displays.



4. Choose Add/Remove Windows Components in the Quick Task bar
5. Choose Application Server
6. Choose Internet Information Services
7. Choose World Wide Web Service See the screen capture on the next page.



8. Click OK, then OK, then OK then Next, then Finish.

## 2.2. Certificate of Authority setup

1. Click the Start Button
2. Click Control Panel
3. Go to Add or Remove Programs
4. Choose Add/Remove Windows Components in the Quick Task bar
5. Choose Certificate Services and click Yes in response to the popup window.

The CA Identifying Information window displays.

Windows Components Wizard

**CA Identifying Information**  
Enter information to identify this CA.

Common name for this CA:  
paquetin

Distinguished name suffix:  
DC=bringsjoy,DC=com

Preview of distinguished name:  
CN=paquetin,DC=bringsjoy,DC=com

Validity period: 5 Years

Expiration date: 6/17/2011 10:27 PM

< Back Next > Cancel Help

6. Enter “paquetin” in the Common name for this CA box, as shown above.
7. Click Next, then Next, then Yes, then Yes to the ASP popup window then click Finish.

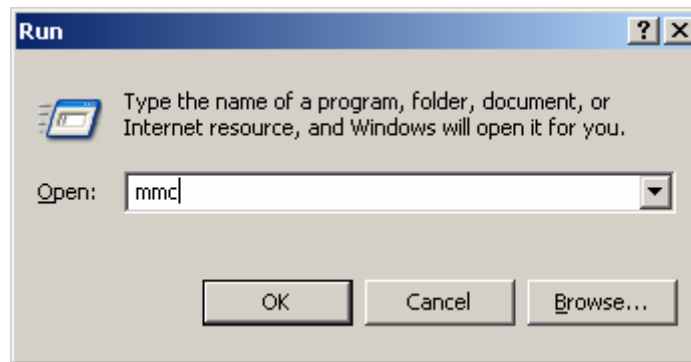
To see if the CA issued a certificate, there are two choices:

8. Quick Way
  - Click Start
  - Click Control Panel
  - Click Administrative tools
  - Choose Certificate AuthorityJump to the last picture in this section.
9. Long Way
  - Opening the Certificates (local computer) snap-in.  
This is the long way of doing it, but this procedure paves the way for other maintenance options if needed later on

To a open a Console window

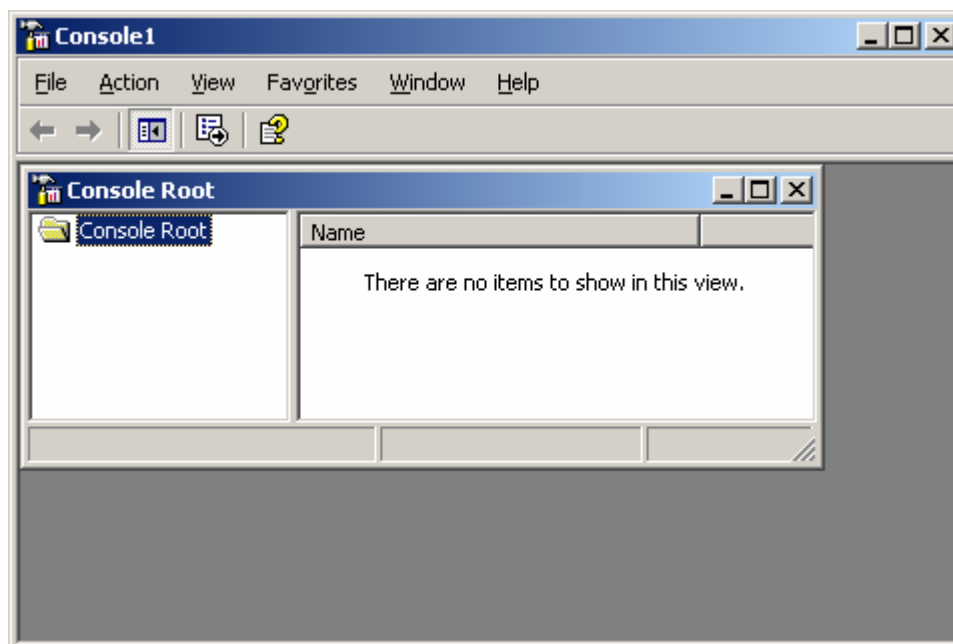
10. Click Start
11. Click Run

The Run window displays



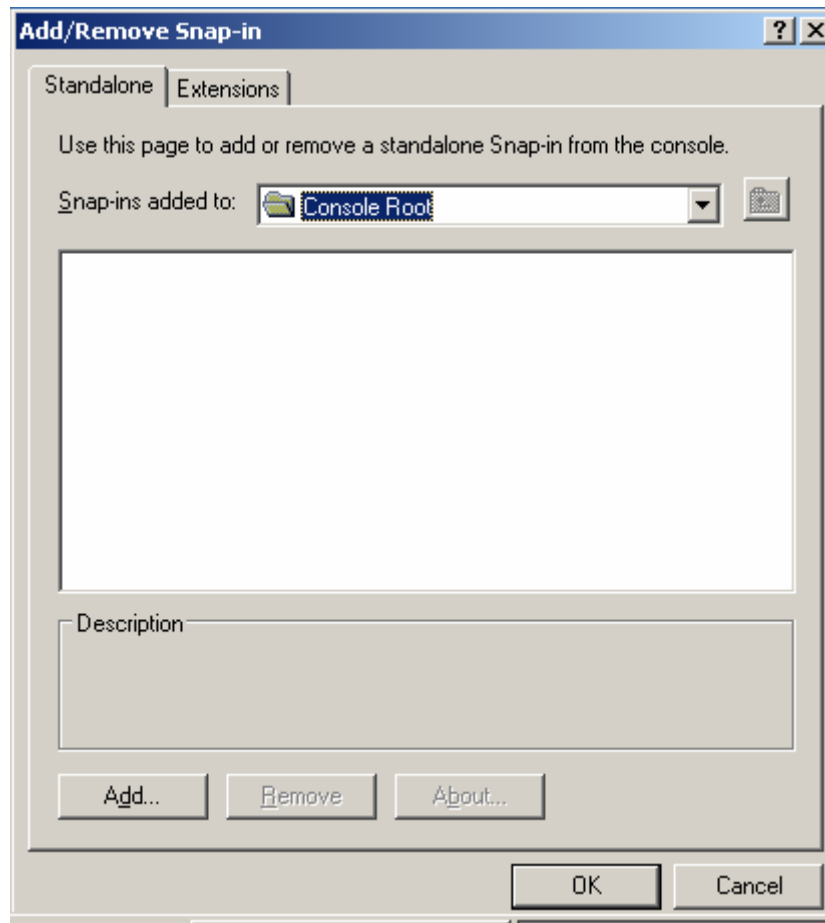
12. Enter mmc in the Open: box as shown above
13. Click OK

The Console window displays



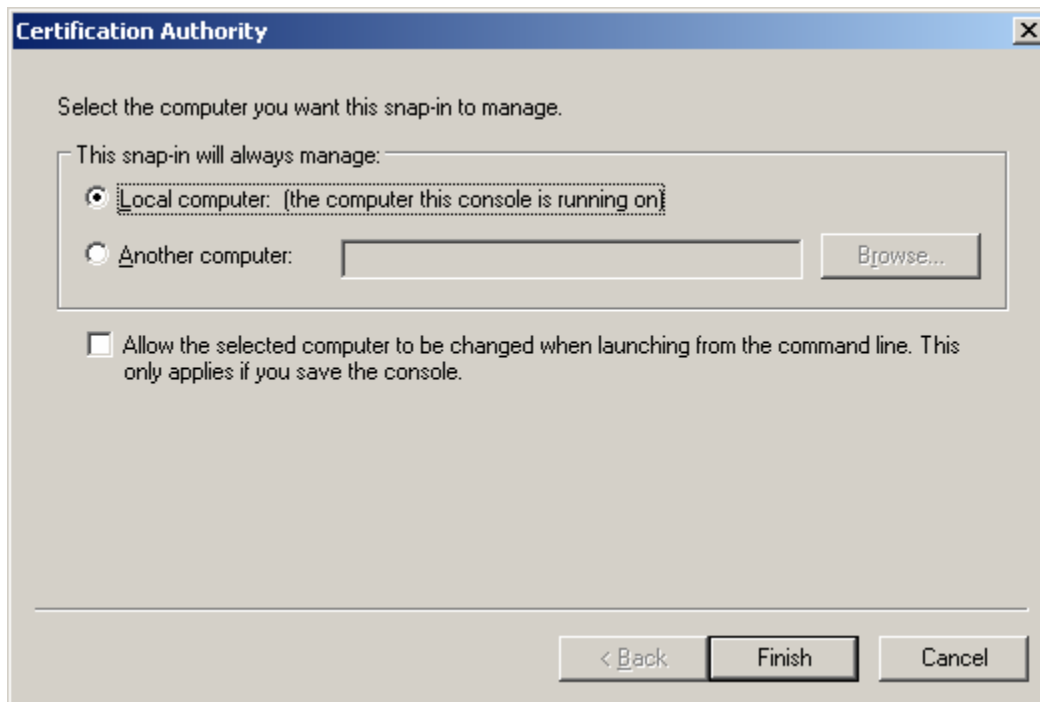
14. From the File menu click Add/Remove Snap-in ...

The Add/Remove Snap-in window displays/

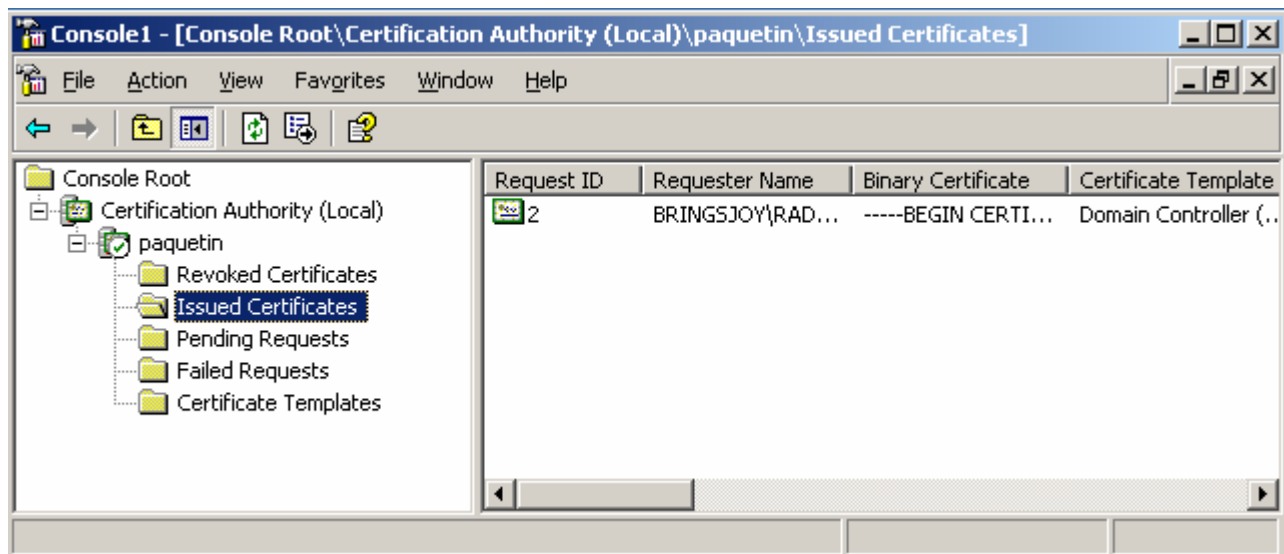


15. Click Add
16. From the list choose Certification Authority then click Add.

The Certification Authority window displays/



17. Click Finish, then Close, then OK

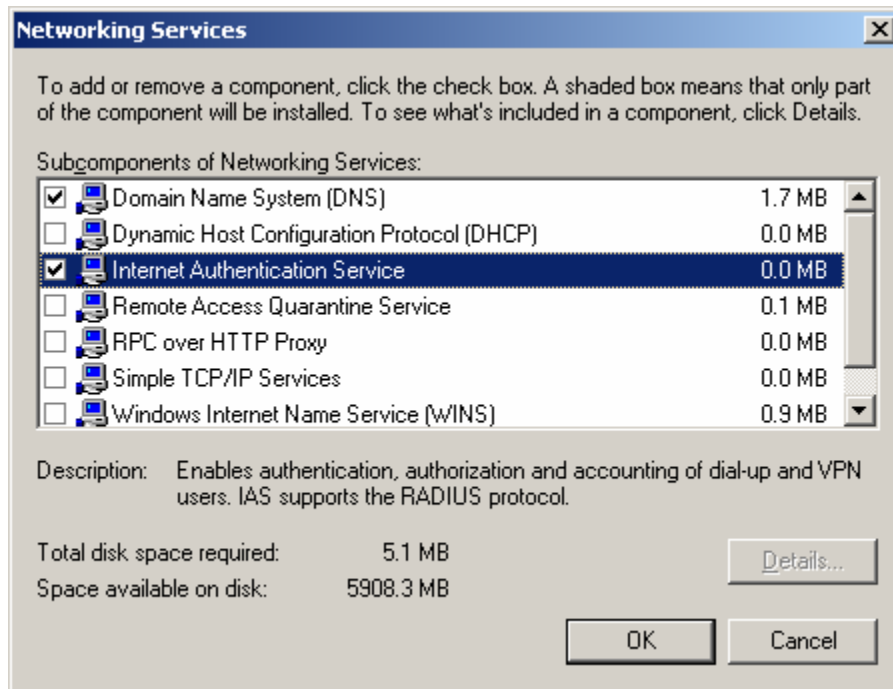


If for some reason, you do not see a certificate, please reboot the machine before continuing

### 3. Setup IAS to configure RADIUS

1. Click Start
2. Click Control Panel
3. Click Add or Remove Programs
4. Choose Add/Remove Windows Components in the Quick Task bar
5. Open details for Networking Services

The Networking Services window displays.



6. Choose Internet Authentication Service
7. Click OK, then Next, then Next]

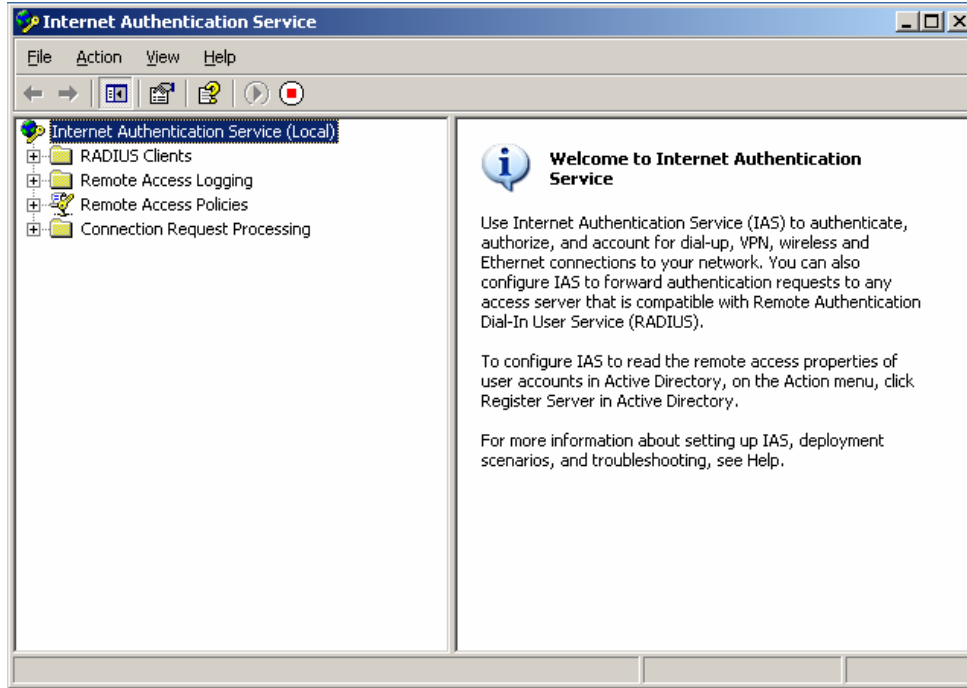
#### 3.1. Setup the RADIUS client

This is accomplished in the IAS MMC, which can be opened on a default installation by

1. Clicking Start
2. Clicking Programs
3. Clicking Administrative Tools
4. Clicking Internet Authentication Service.



The Internet Authentication Service window displays



5. Right click on RADIUS Clients and select 'New RADIUS Client'

The New RADIUS Client window displays

**New RADIUS Client**

Name and Address

Type a friendly name and either an IP Address or DNS name for the client.

Friendly name:

Client address (IP or DNS):

< Back   Next >   Cancel

6. Enter Friendly name and IP address (or range) of access point and click Next  
This is where you can allow for a group of AP's to be managed under 1 RADIUS server. With the above configuration of 172.16.1.0/24, we can add several AP's as needed and they will connect to the RADIUS server as long the AP's are on the same network/subnet.

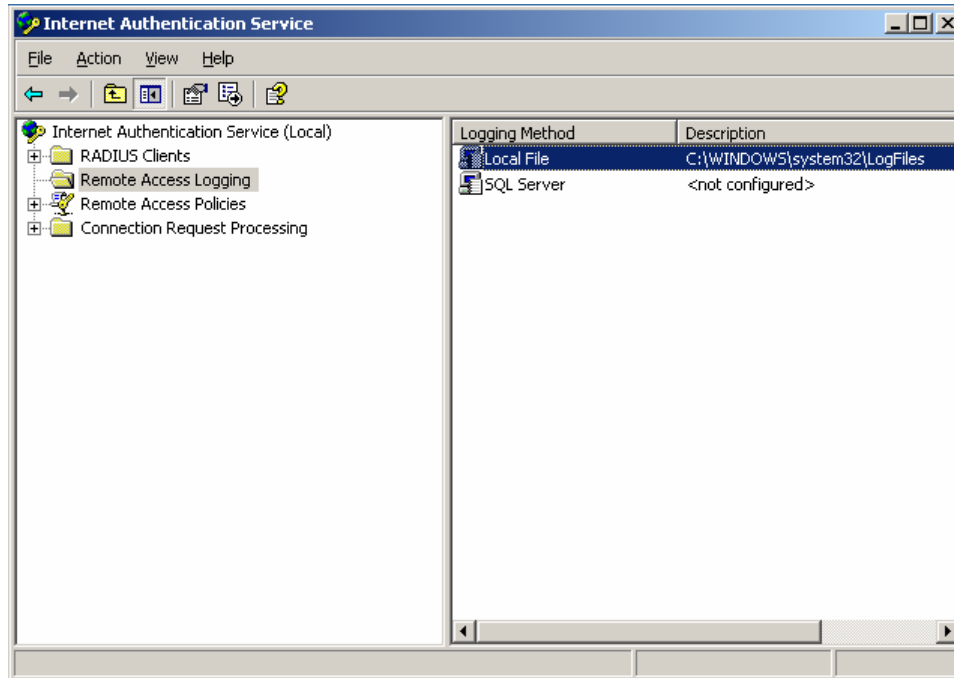
The Additional Information window displays

The screenshot shows a Windows dialog box titled "New RADIUS Client" with a close button in the top right corner. The dialog has a tab labeled "Additional Information". Below the tab, there is a line of text: "If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client." Below this text are four fields: 1. "Client-Vendor:" with a dropdown menu showing "RADIUS Standard". 2. "Shared secret:" with a text box containing "xxxxxxx". 3. "Confirm shared secret:" with a text box containing "xxxxxxx". 4. A checked checkbox labeled "Request must contain the Message Authenticator attribute". At the bottom of the dialog are three buttons: "< Back", "Finish", and "Cancel".

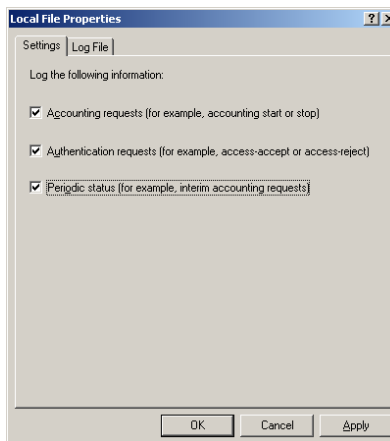
7. Select 'RADIUS Standard'(Default) from the Client-Vendor: drop-down list
8. Enter your pre-shared key in both the Shared secret: box and Confirm shared secret: boxes.  
In our scenario it is "qaz123". This key should be as long as possible for production purposes, a random character generator is recommended.
9. Check Request must contain the Message Authenticator attribute.

### 3.2. Configure logging

1. Highlight Remote Access Logging on the IAS tree in the left pane.
2. Double click Local File in the right pane



The Local File Properties window displays.

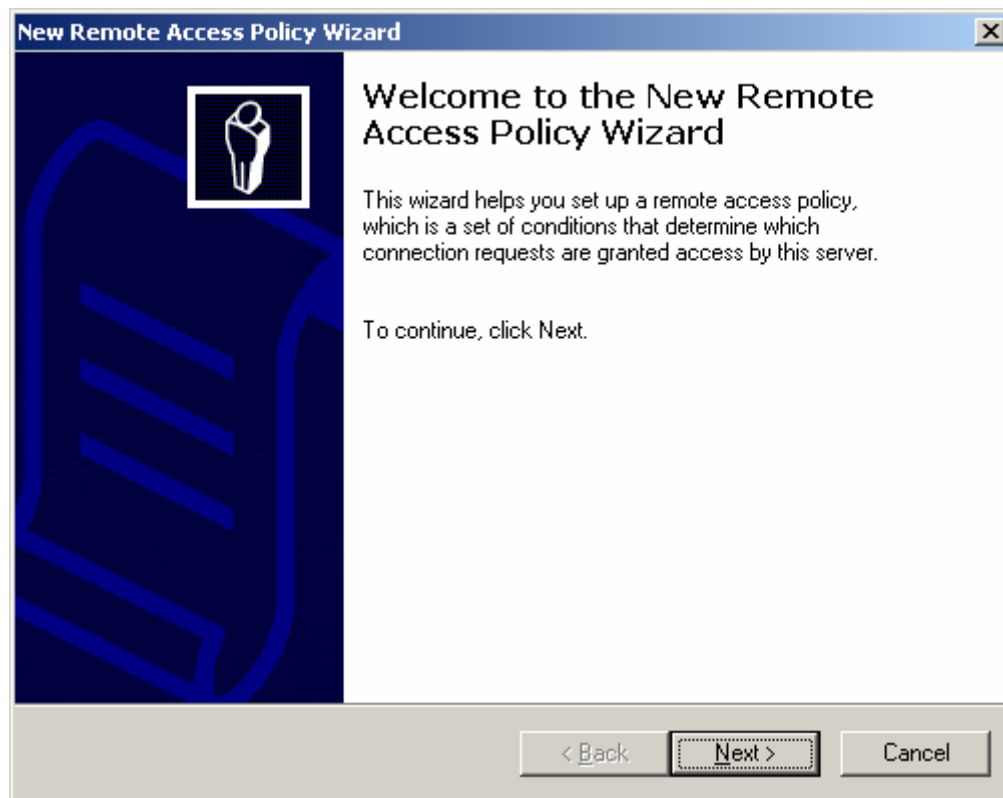


3. Select all 3 check boxes: Accounting requests, Authentication requests, and Periodic status for full logging to log files.  
To find these logs, you can use the Windows Search utility specifying for "IN\*.LOG". These logs are very useful in the process of troubleshooting.

### 3.3. Setup a Remote Access Policy

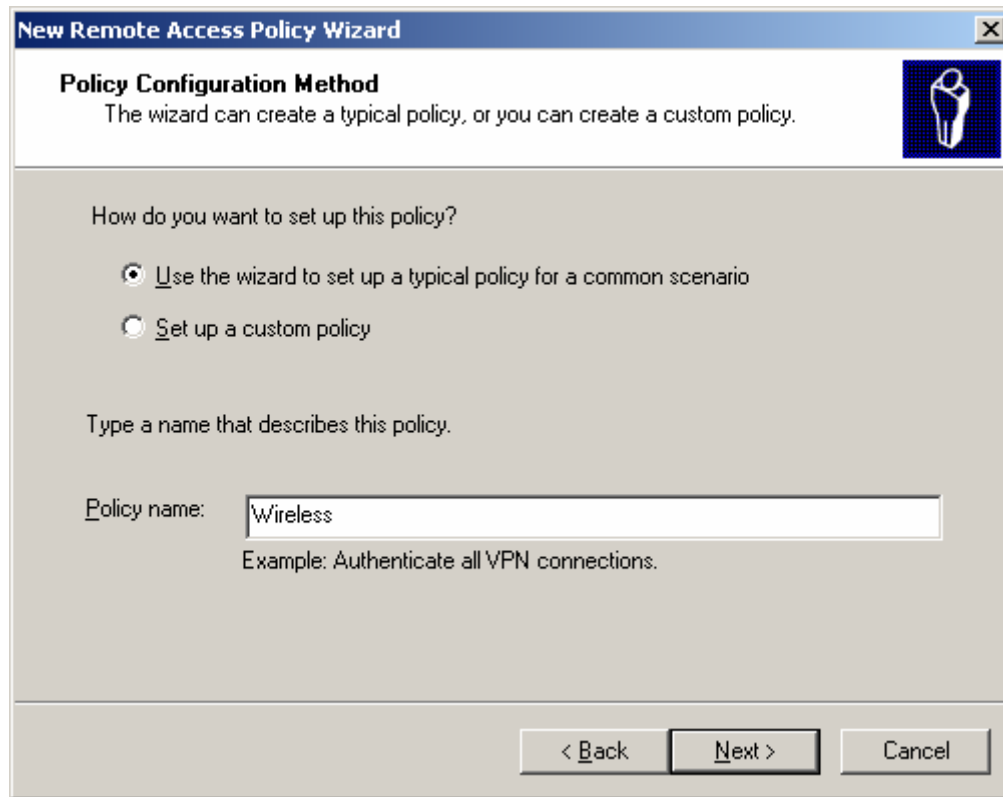
1. Right click on Remote Access Policies
2. Select 'New Remote Access Policy'

The New Remote Access Policy Wizard displays.



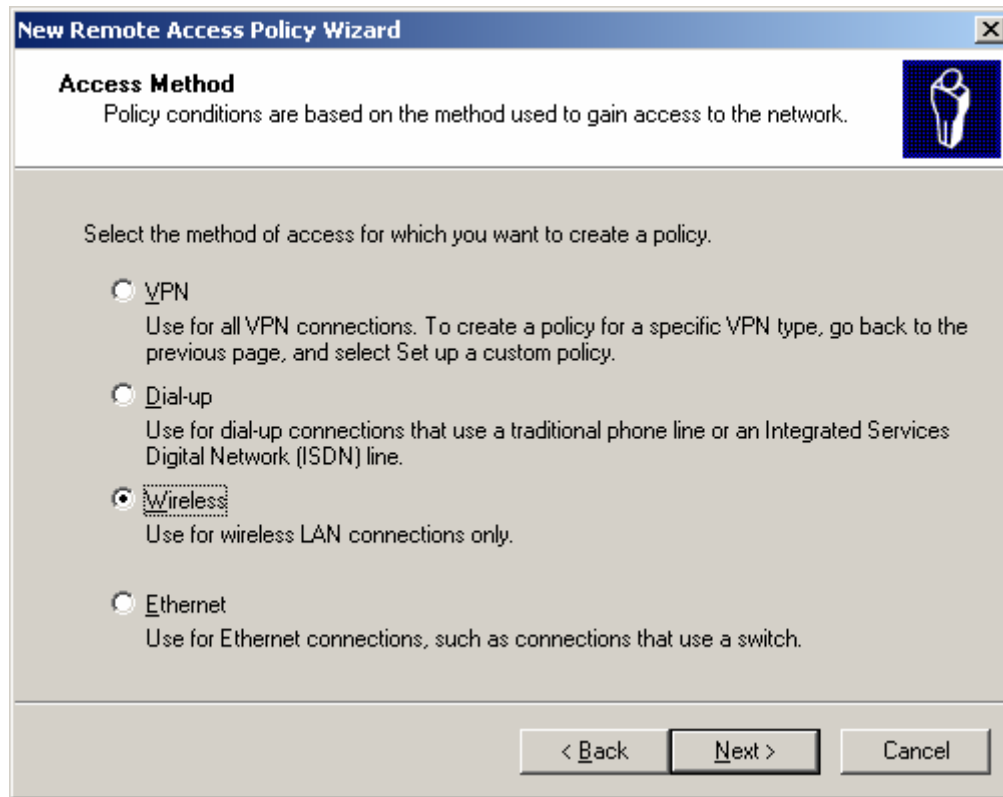
3. Click Next

The Policy Configuration Method window displays.



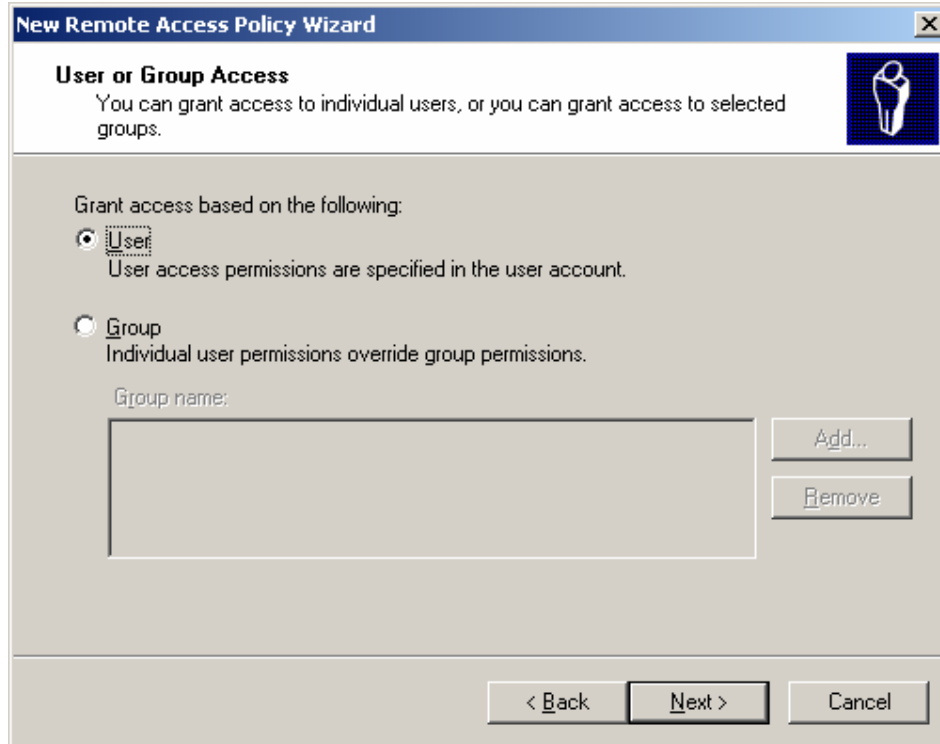
4. Select Use the wizard to set up a typical policy for a common scenario
5. Enter a Policy name  
In our scenario it is Wireless
6. Click Next

The Access Method window displays.



7. Select Wireless
8. Click Next

The User or Group Access Method window displays.



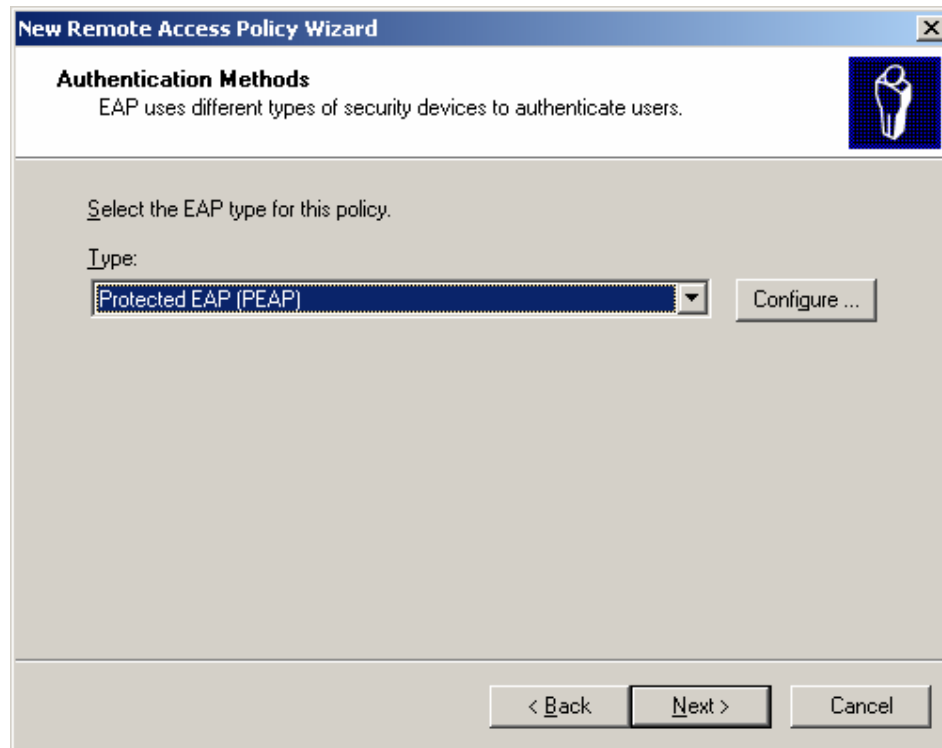
9. Select User to grant level access

For simplicity sake, we are using the user option, but for management, it is best to create group policies

10. Click Next.

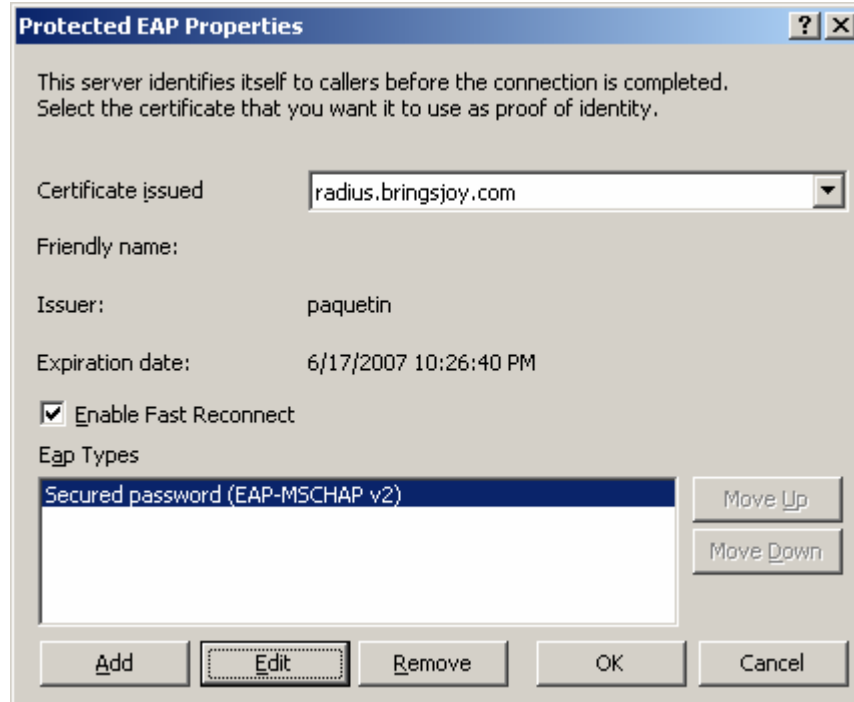


The User or Group Access Method window displays.



11. Select Protected EAP (PEAP) from the drop-down list.  
It should appear as the default value.
12. Click Configure ...

The User or Group Access Method window displays.



13. Ensure the correct Certificate issue option is selected.
14. Select the Enable Fast Reconnect check box
15. Optionally, you may
  - Select the EAP Type “Secured password (EAP-MSCHAPv2)”
  - Click Edit, and
  - Adjust options as desired.
16. When done, click OK, then Finish

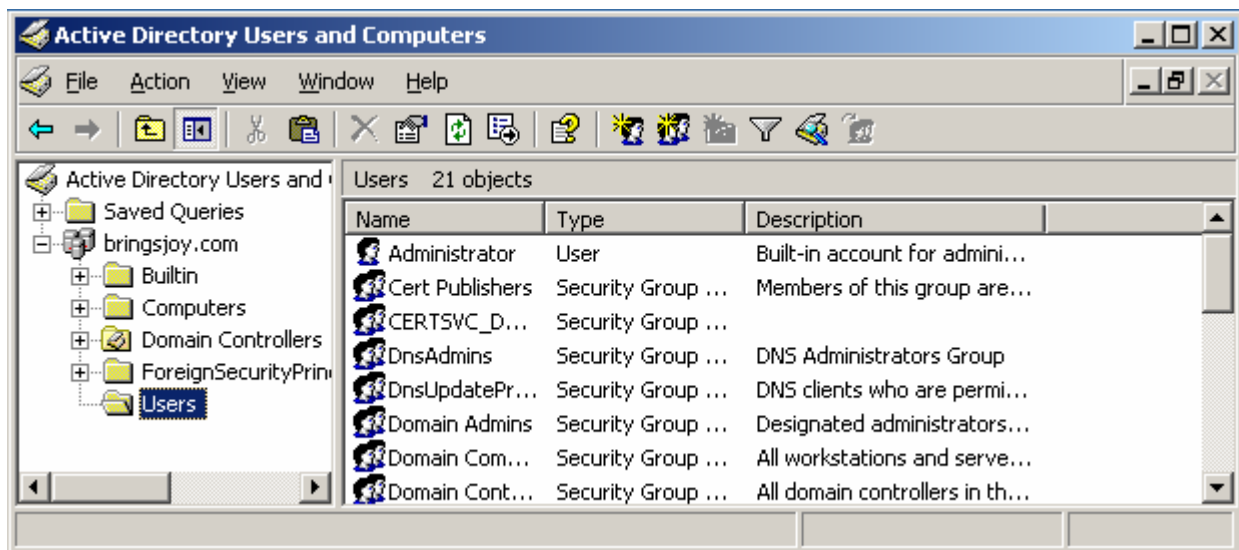
Later on, if needed you can configure scheduled hours or days of the week in which connections are allowed or denied.

### 3.4. Configure user accounts

The final step required on the server is to configure a user account to be used with the RADIUS account. This can be an existing AD account, or you can add a group to be used exclusively for wireless access authentication.

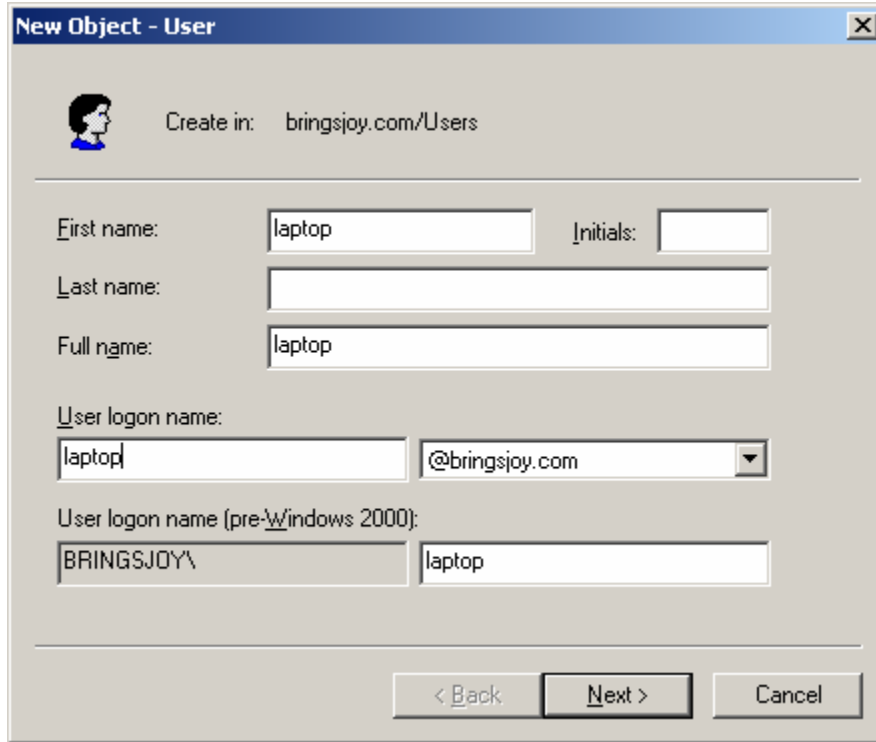
1. Click Start
2. Click Programs
3. Click Administrative Tools
4. Click Active Directory Users and Computers

The Active Directory Users and Computers window displays.



5. Select the domain to be used for the wireless users.
6. Right click on the User folder
7. Select New
8. Select User.

The New Object – User window displays.



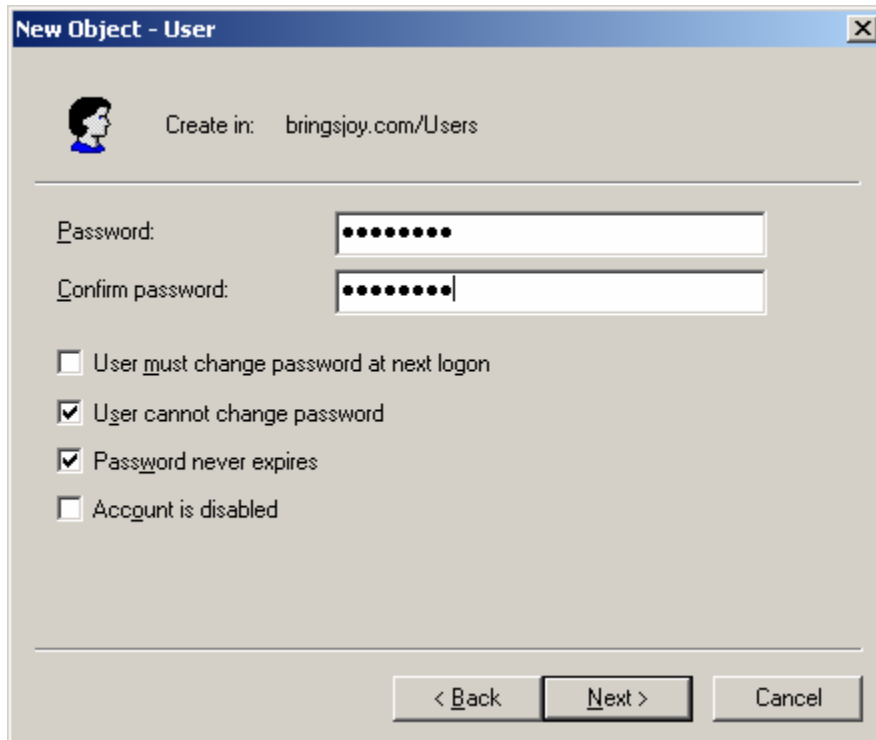
The screenshot shows the 'New Object - User' dialog box. At the top, it says 'Create in: bringsjoy.com/Users'. Below that, there are several input fields:

- First name: laptop
- Initials: (empty)
- Last name: (empty)
- Full name: laptop
- User logon name: laptop @bringsjoy.com
- User logon name (pre-Windows 2000): BRINGSJOY\laptop

At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

9. Enter the user information as shown above.
10. Click Next.

11. Enter “!qwerty1” in both the Password: and Confirm password: boxes  
It has to be VERY secure so we are using text and number
12. Deselect the checkbox User must change password at next logon
13. Select the checkboxes User cannot change password and Password never expires
14. Click Next.



**New Object - User**

Create in: bringsjoy.com/Users

Password: [masked]

Confirm password: [masked]

User must change password at next logon

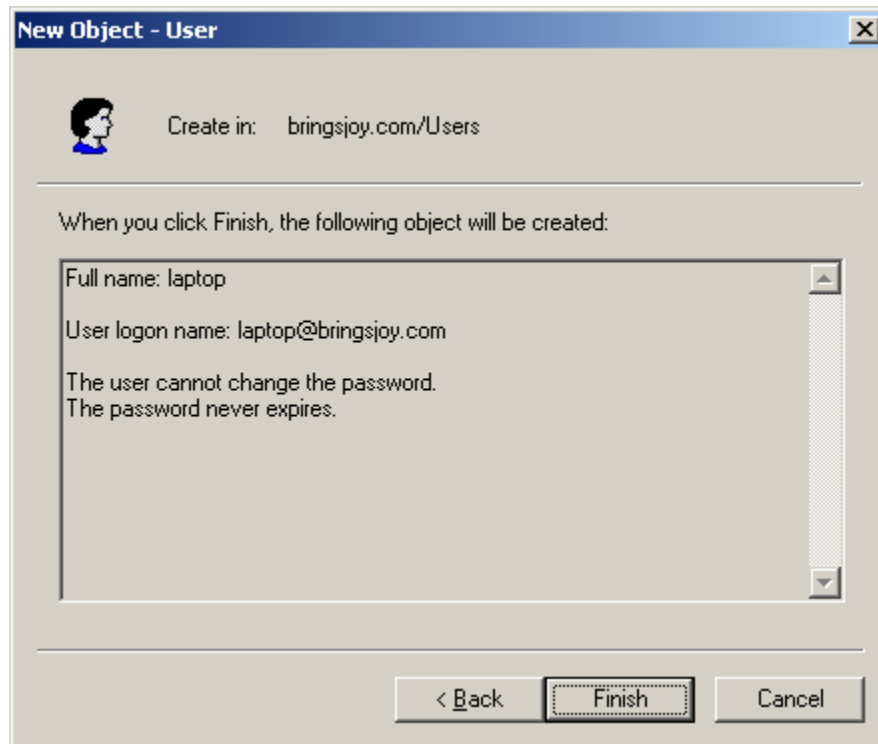
User cannot change password

Password never expires

Account is disabled

< Back   **Next >**   Cancel

The confirmation window displays.

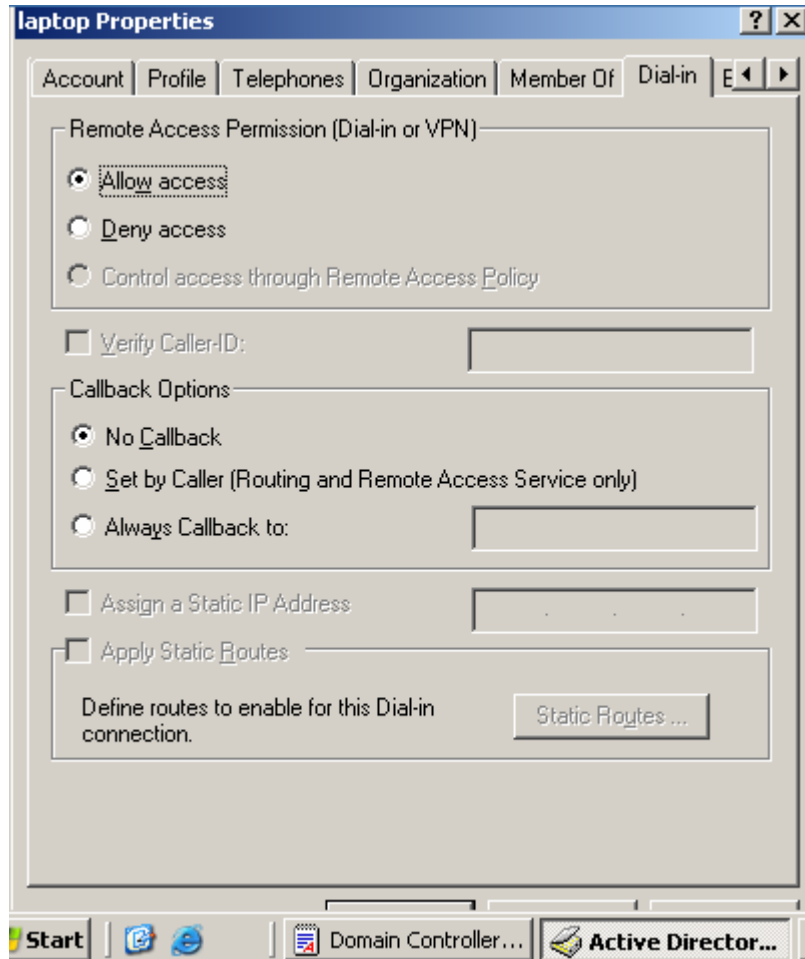


15. Click Finish.

16. Right click on the new user

17. Select Properties

The laptop Properties window displays



18. Select the Dial-in tab

19. Select Allow access.

We are done with the server side configuration.