Configuring EAP for Wireless Network Connectivity

By Victor Zapata

Requirements:

1. **Windows 2000 Domain Controller** Service Pack 2 with hotfixes Q306260 and Q304347 – OR – Service Pack 3
2. **Enterprise Certificate Authority**
3. **Windows 2000 IAS Server (RADIUS)** Service Pack 2 with hotfix Q304697 – OR – Service Pack 3
4. **Windows XP/2000 client** – with computer and user certificates

304347 Server Does Not Make EAP-OE Connection to LAN If a User Is Not Logged On
http://support.microsoft.com/?id=304347

306260 Cannot Modify Dial-In Permissions for Computers That Use Wireless
http://support.microsoft.com/?id=306260

304697 Some Wireless Values for the RADIUS Attributes Are Not Available
http://support.microsoft.com/?id=304697

Outline:

I. Installing Enterprise Certificate Server

II. Installing Computer Certificate on IAS Server

III. Installing Certificates on Client
- a. Install computer certificate
- b. Install user certificate
- c. Configure Automatic Certificate Enrollment via Group Policy

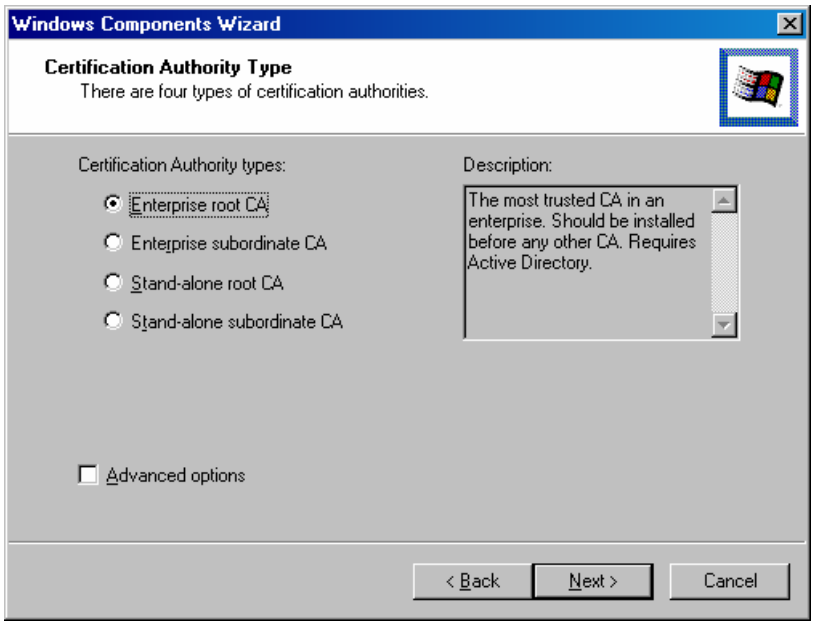
IV. Configuring IAS Server
- a. Register service in Active Directory
- b. Add RADIUS client
- c. Create RAS Policy for 802.1x authentication using EAP
- d. Configure dial-in permissions for domain account

V. Configuring the Client for 802.1x authentication

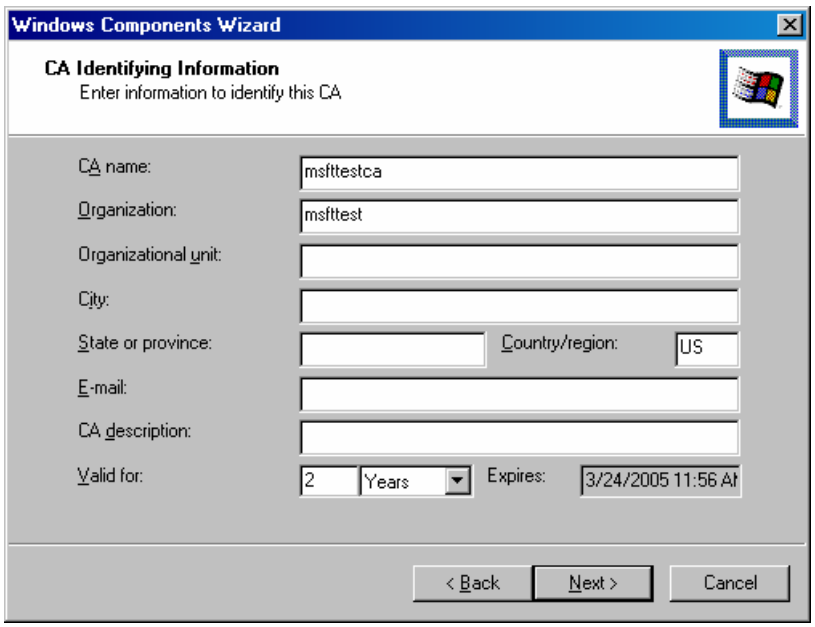
VI. Configuring Access Point for 802.1x authentication (Cisco 340/350)

I. Installing Enterprise Certificate Server

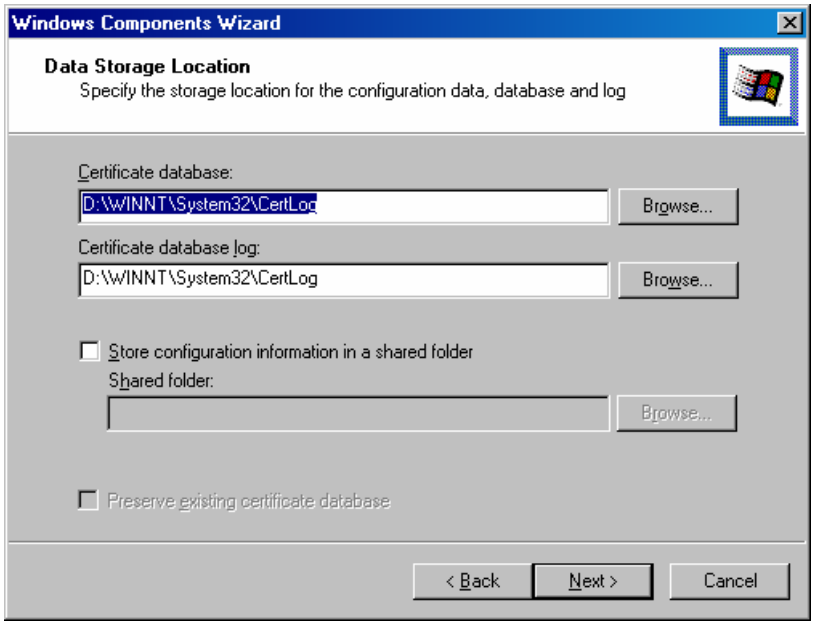
1. Install Certificate Services from the “Add Remove Programs” control panel
2. Select “Enterprise root CA” then click “Next”



3. Enter pertinent information to identify the CA, then click “Next”

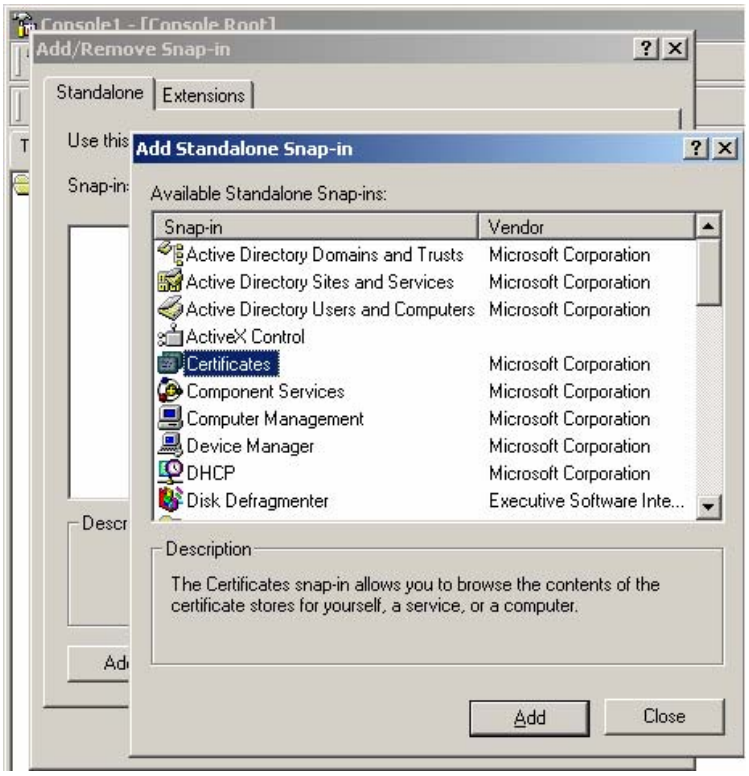


4. A “CertLog” directory is created in %Systemroot%\System32 for certificate database storage, click “Next” then “Finish”

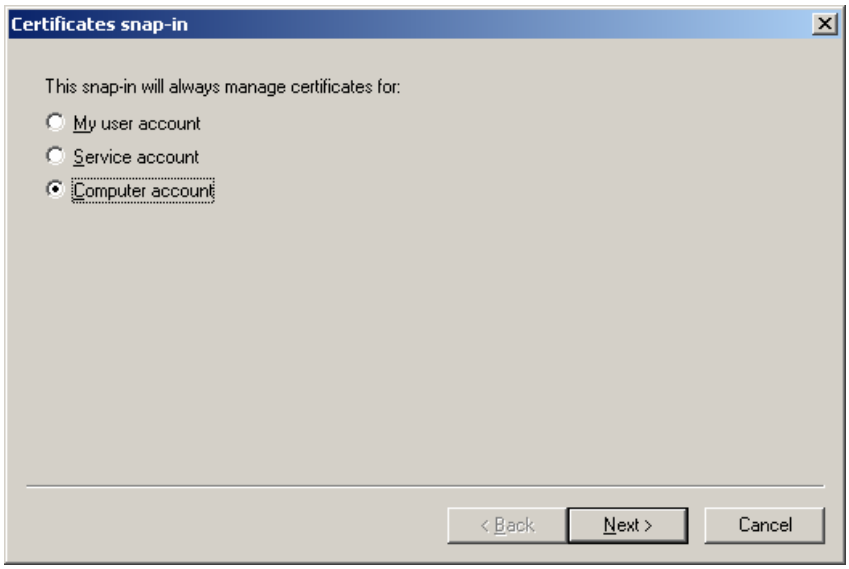


II. Installing Computer Certificate on IAS Server

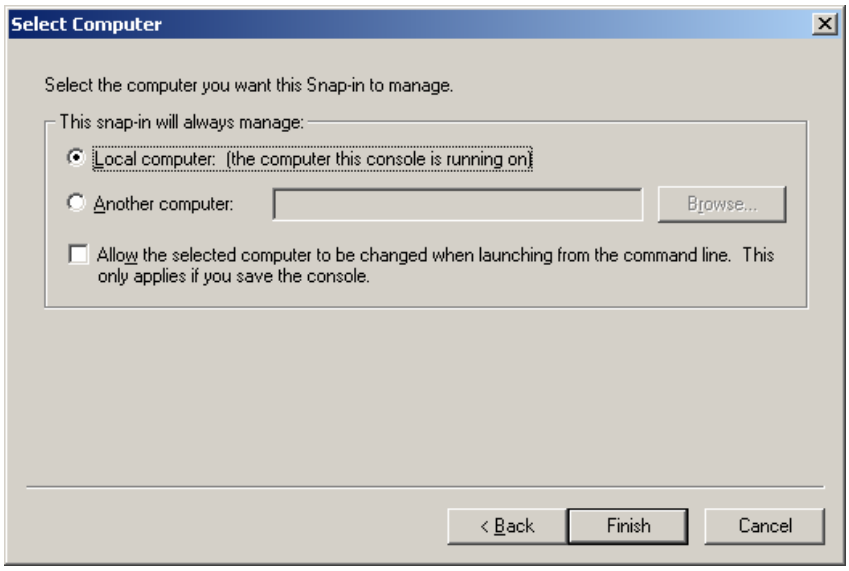
1. Open a “Certificates” MMC by click on “START, then “RUN”, then type “MMC” and click “OK”
2. Click “Console” in the file menu, then select “Add\Remove Snap-in”
3. Click “Add” to add a snap-in
4. Select “Certificates” from the list of snap-ins



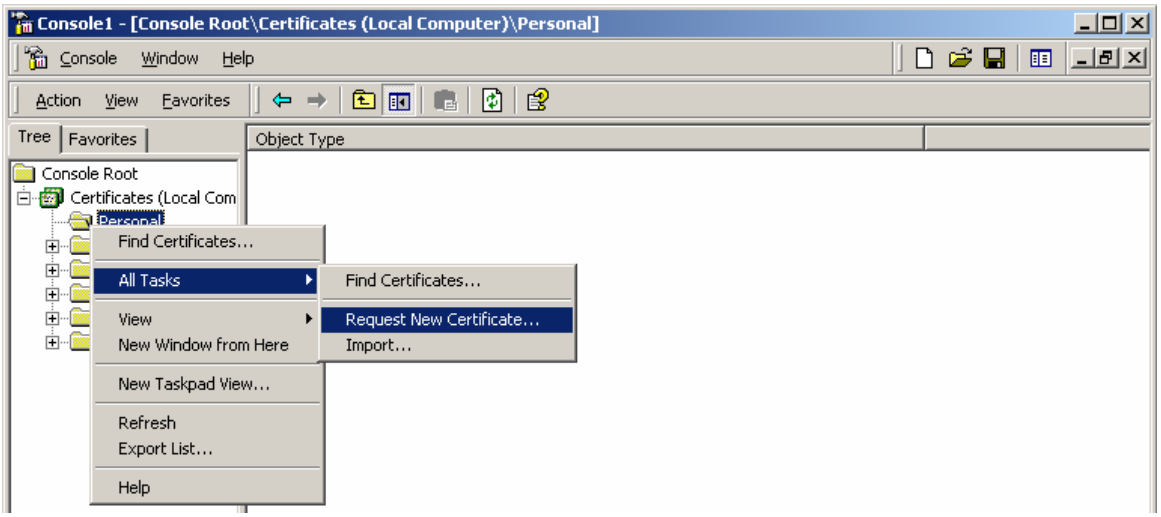
5. Select “Computer account”



6. Select “Local computer”

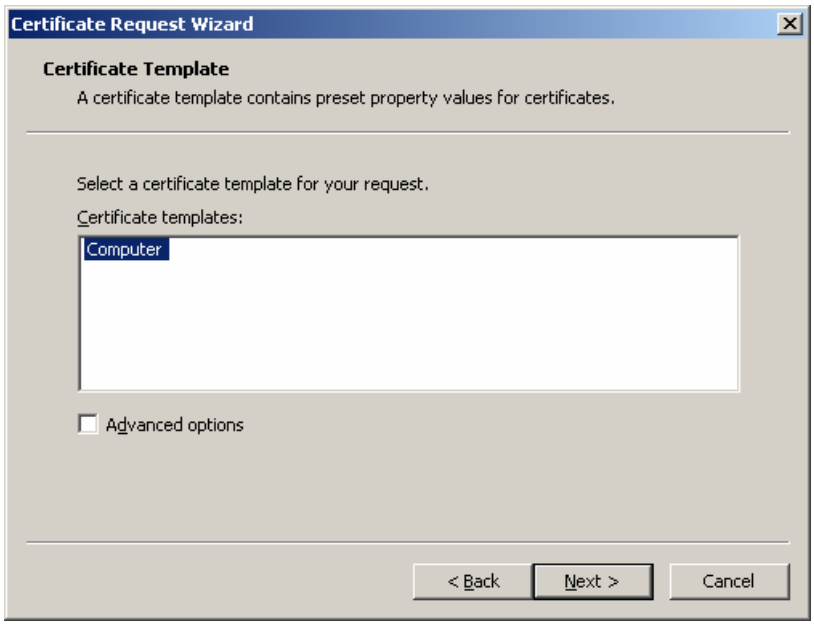


7. To request a certificate from the CA, right-click the “Personal” container, select “All Tasks, then “Request New Certificate”

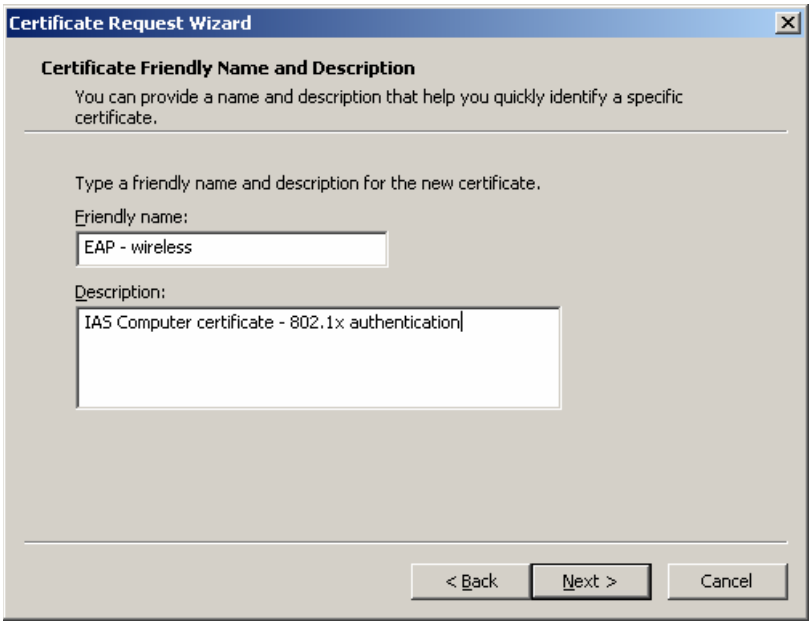


8. click “Next” on the Welcome screen

9. select the “Computer” certificate template



10. create a friendly name to assist in identifying the intended purpose for the computer certificate, then click “Next”



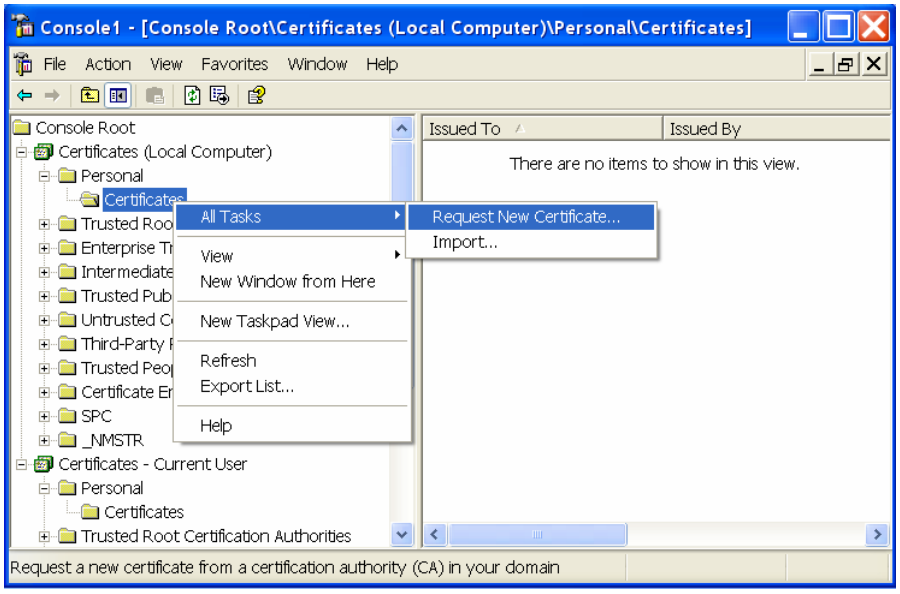
11. click “Finish”


Certificate Request Wizard
Completing the Certificate Request Wizard
You have successfully completed the Certificate Request wizard.
You have specified the following settings:
Friendly Name EAP - wireless
Computer Name ISASVR
Certificate Template Computer
CSP Microsoft RSA SChannel Cryptog
< Back
Finish
Cancel

III. Installing Certificates on Client

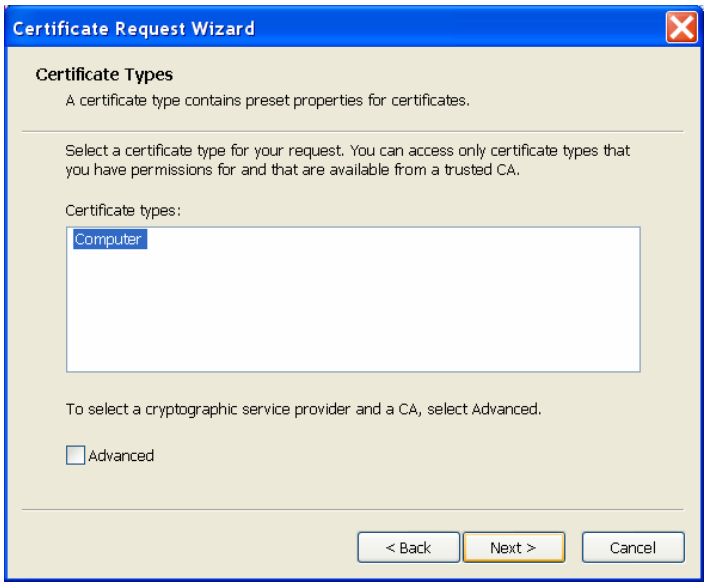
A. Install Computer Certificate

1. Open a “Certificates” MMC by click on “START, then “RUN”, then type “MMC” and click “OK”
2. Click “File” in the file menu, then select “Add\Remove Snap-in”
3. Click “Add” to add a snap-in
4. Select “Certificates” from the list of snap-ins
5. Select “Computer account” then click “Next”
6. Select “Local Computer” then click “Finish”
7. To request a certificate from the CA, right-click the “Personal” container, in the ***Local Computer*** certificate snap-in , select “All Tasks, then “Request New Certificate”

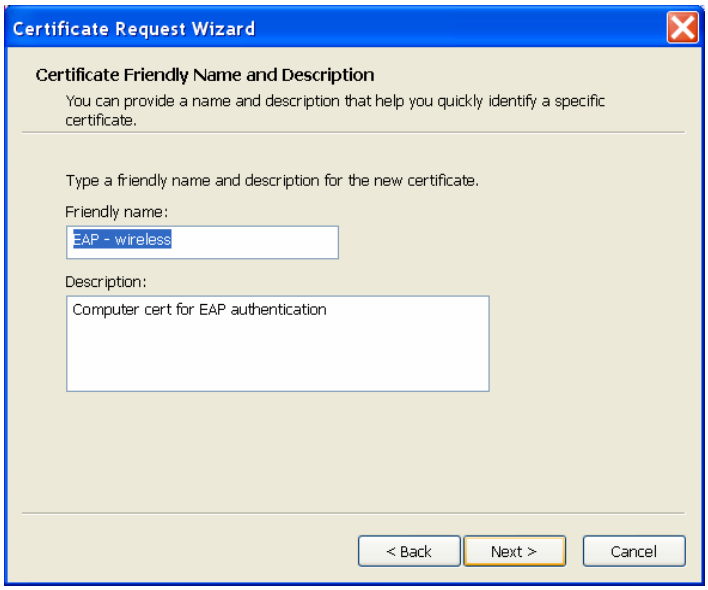


8. click “Next” on the welcome screen

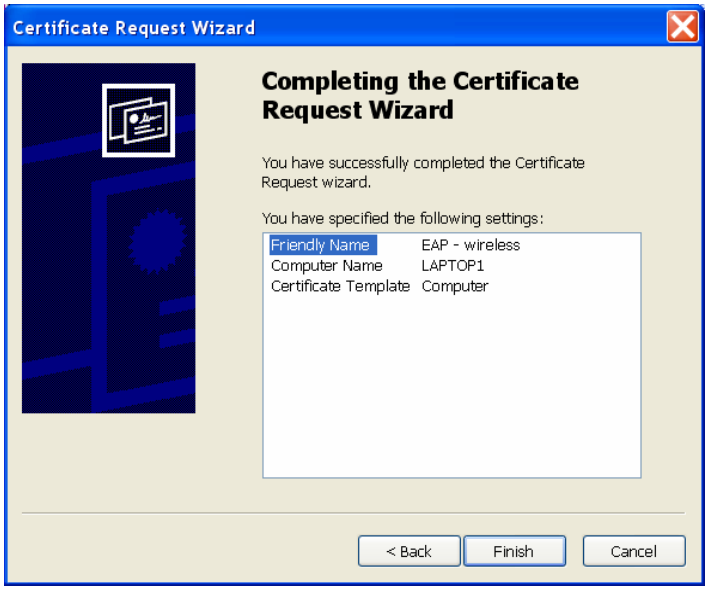
9. select the “Computer” certificate template



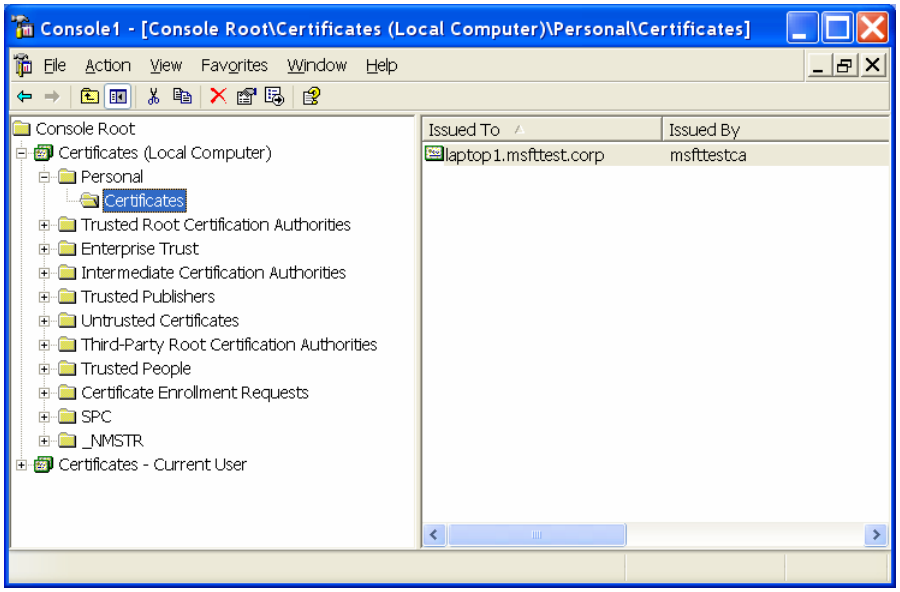
10. create a friendly name to assist in identifying the intended purpose for the computer certificate, then click “Next”



11. click “Finish”

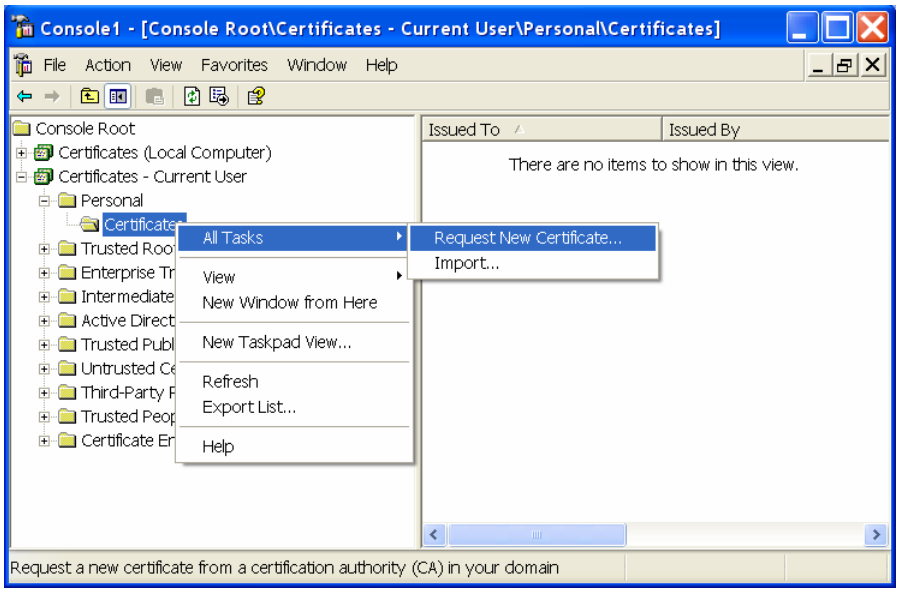


12. you should now see a computer certificate in the list

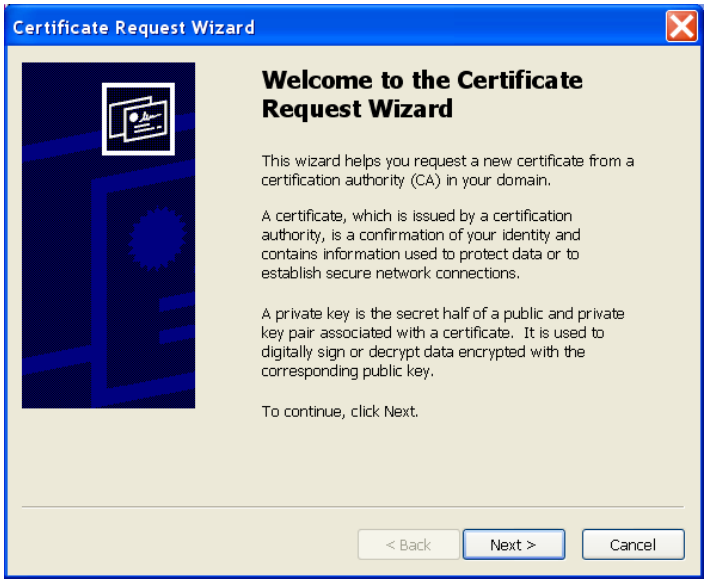


B. Install Computer Certificate

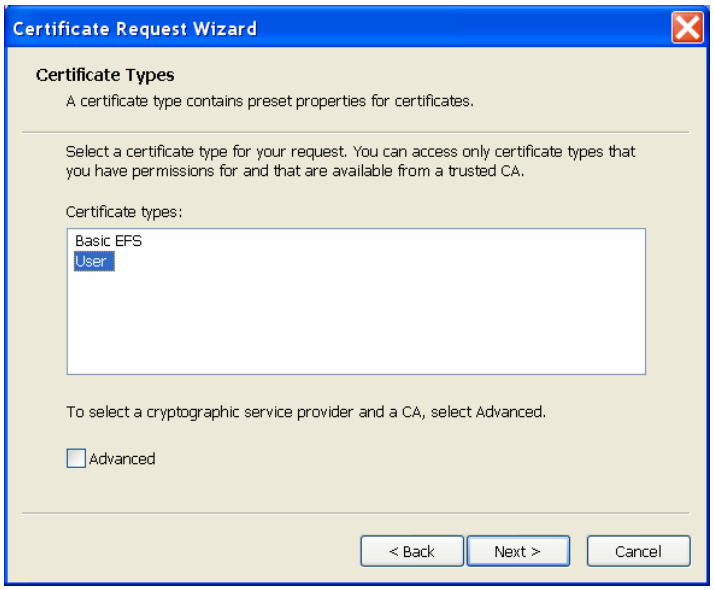
1. Open a “Certificates” MMC by click on “START, then “RUN”, then type “MMC” and click “OK”
2. Click “File” in the file menu, then select “Add\Remove Snap-in”
3. Click “Add” to add a snap-in
4. Select “Certificates” from the list of snap-ins
5. Select “My user account” then click “Finish”
6. To request a certificate from the CA, right-click the “Personal” container, in the ***Current User*** certificate snap-in , select “All Tasks, then “Request New Certificate”



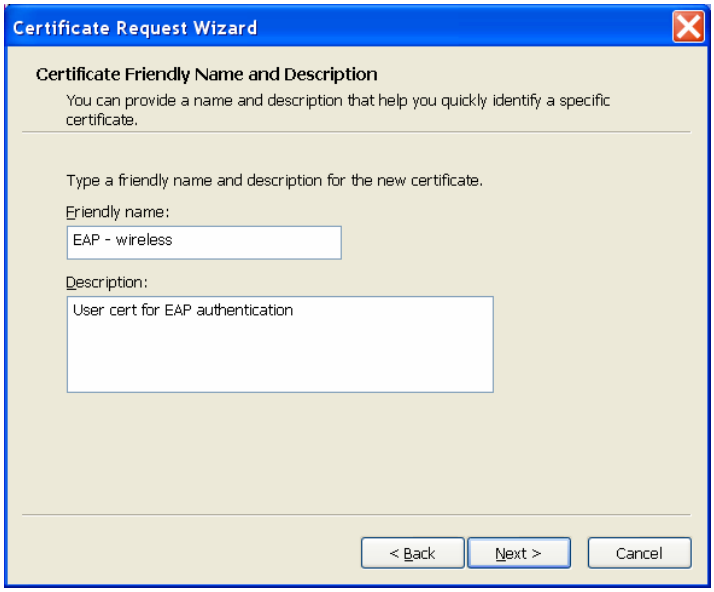
7. click “Next” on the Welcome screen



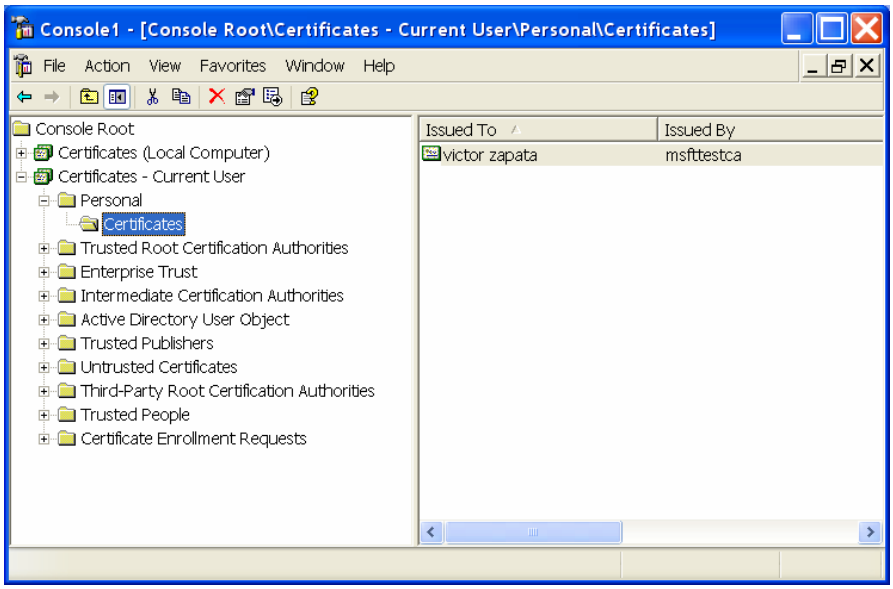
8. Select “User” as the requested certificate type



9. enter a friendly name to assist in identifying the intended purpose for the computer certificate, then click “Next”



10. you should now see a user certificate in the list



C. Configure Automatic Certificate Enrollment via Group Policy

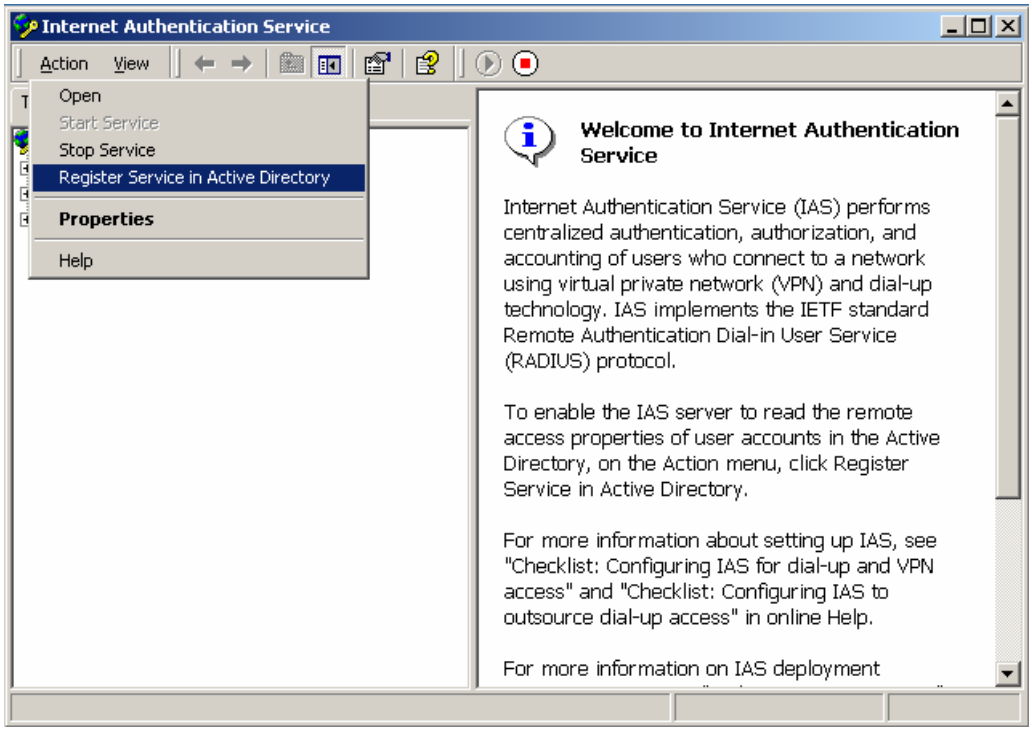
1. Click the domain object and then right-click “Properties”
2. Click the Group Policy tab, and then click Edit
3. Expand the Computer Configuration object, and locate the following object: Windows Settings\Security Settings\Public Key Policies\Automatic Certificate Request
4. Right-click the object, click New, and then click Automatic Certificate Request

5. Click the Computer object, and the click Next
6. Click the appropriate Certificate Authority (CA), click “Next”, and then “Finish”
7. Verify that the certificate enrollment object has appeared

IV. Configuring IAS Server

A. Register Service In Active Directory

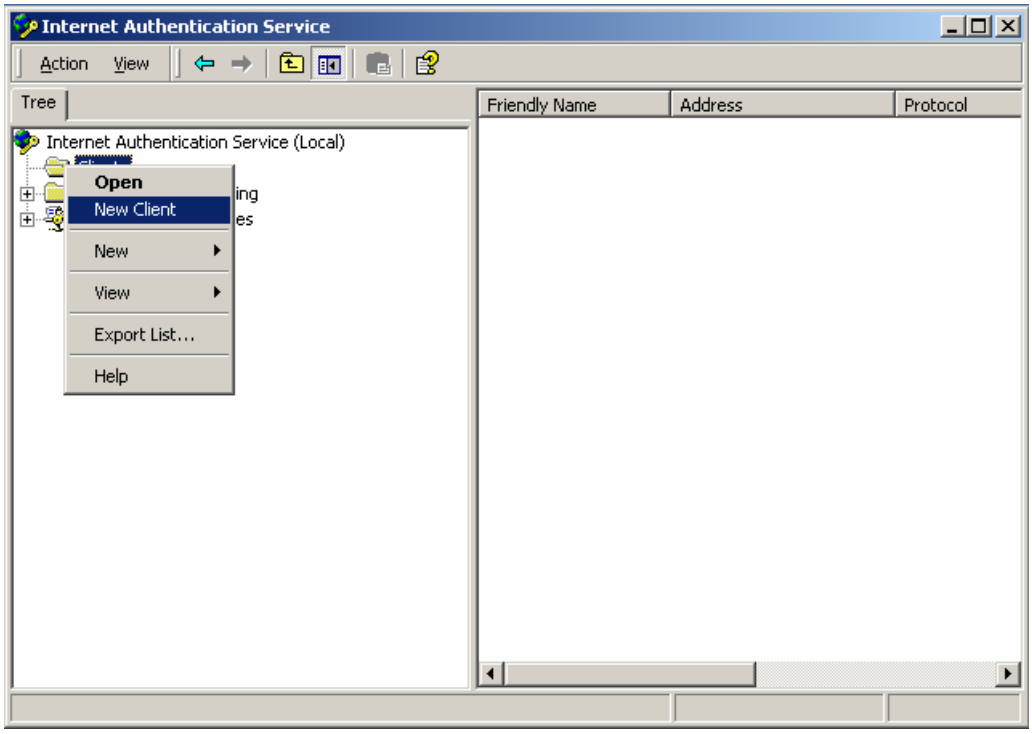
1. click “Action” in the file menu and select “Register Service in Active Directory”
   a. This can also be accomplished using the following NETSH command: **netsh ras add registeredserver**



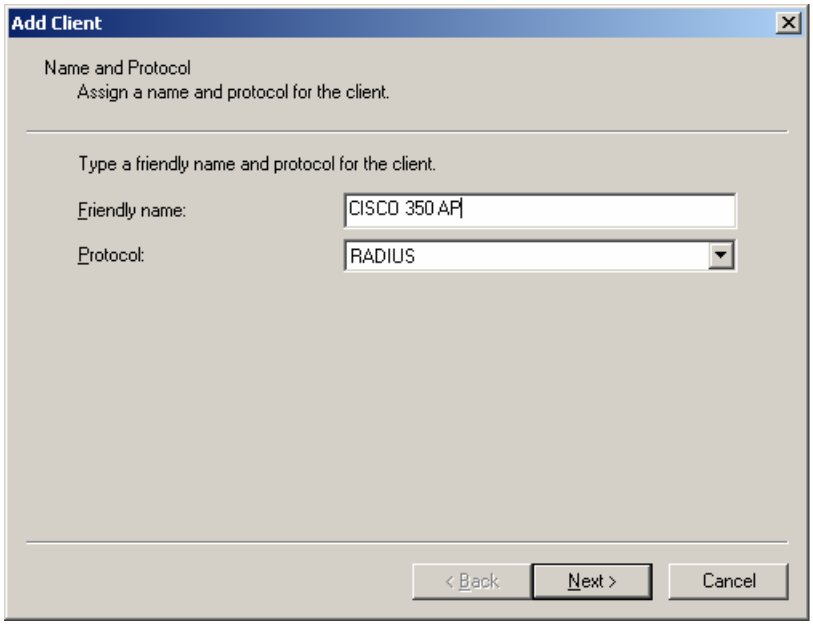
2. click “OK” to authorize IAS to access user’s dial-in permissions

B. Add RADIUS client (client = access point)

1. right-click the “Clients” container and select “New Client”

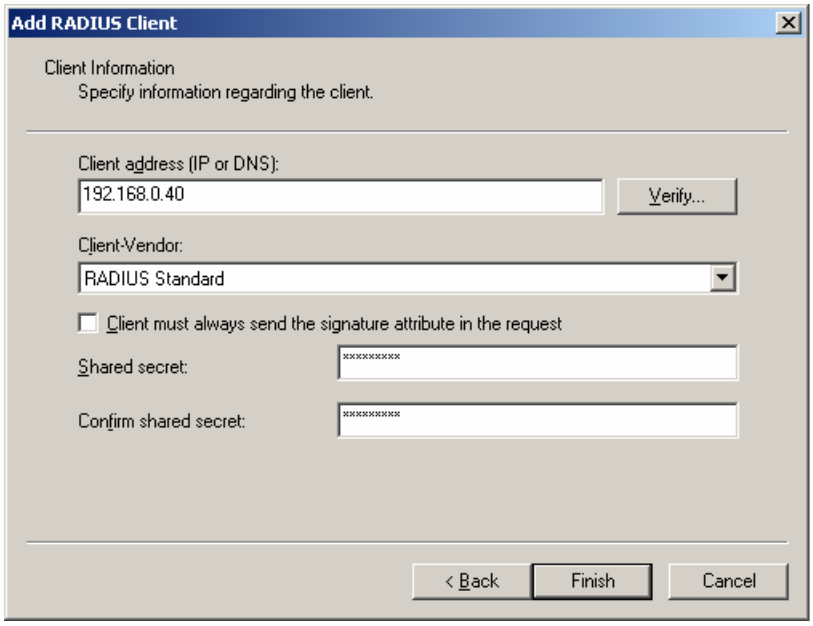


2. enter friendly name for Access Point (AP) and specify RADIUS as the protocol to use, then click “Next”

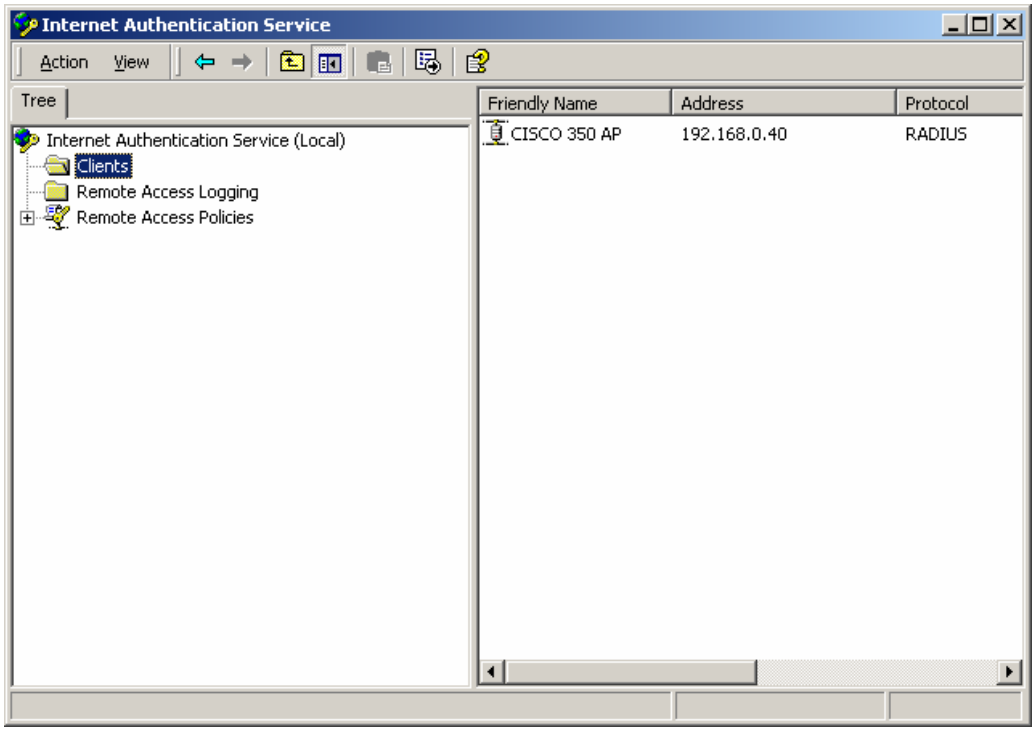


3. enter the AP’s IP address and create a shared secret, then click “Next”

* enabling the “Client must always send the signature attribute in the request” option is not necessary as this is already performed when using EAP

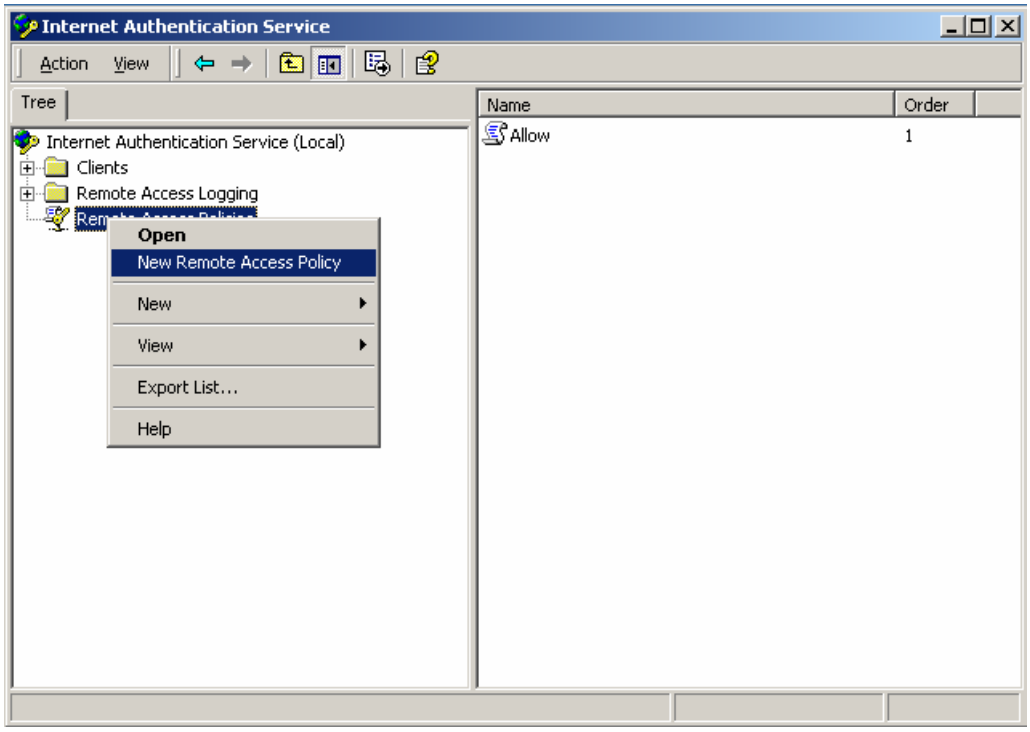


4. you should now see the AP in the client list

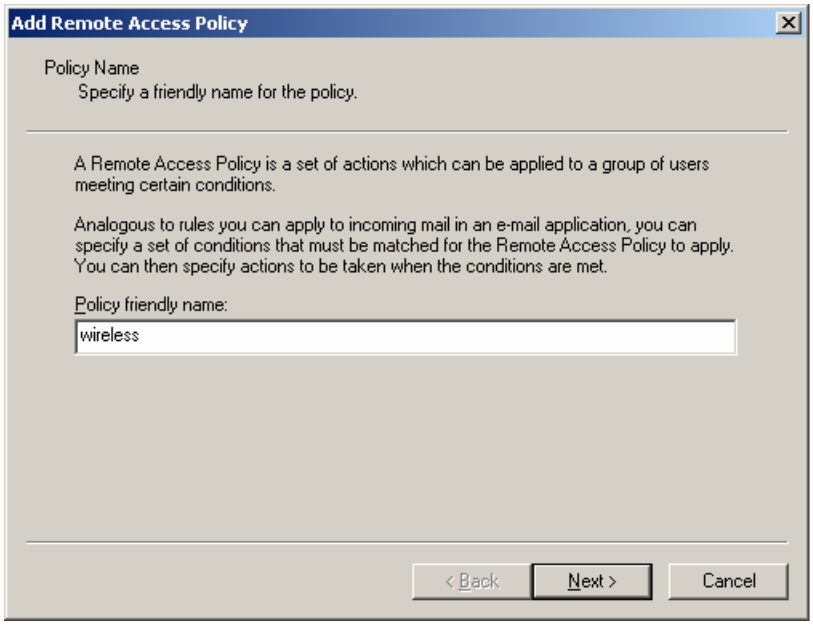


C. Create RAS Policy for 802.1x authentication using EAP

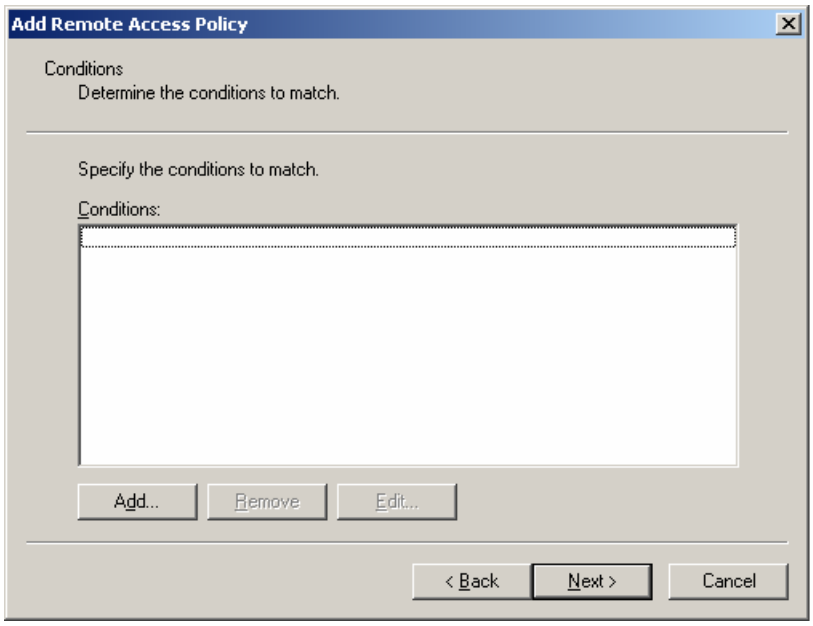
1. right-click “Remote Access Polices” and select “New Remote Access Policy”



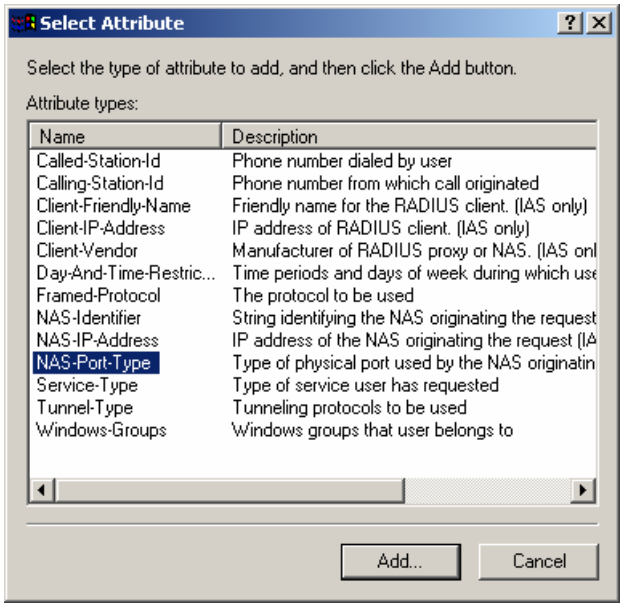
2. enter friendly name for the RAS Policy, then click “Next”



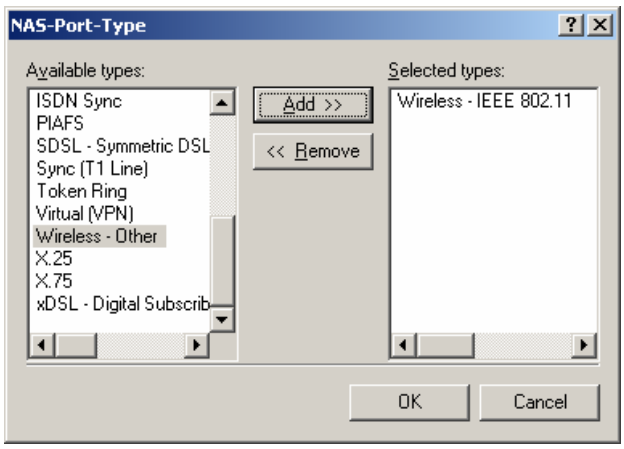
3. click “Add” to specify criteria for RAS connection’



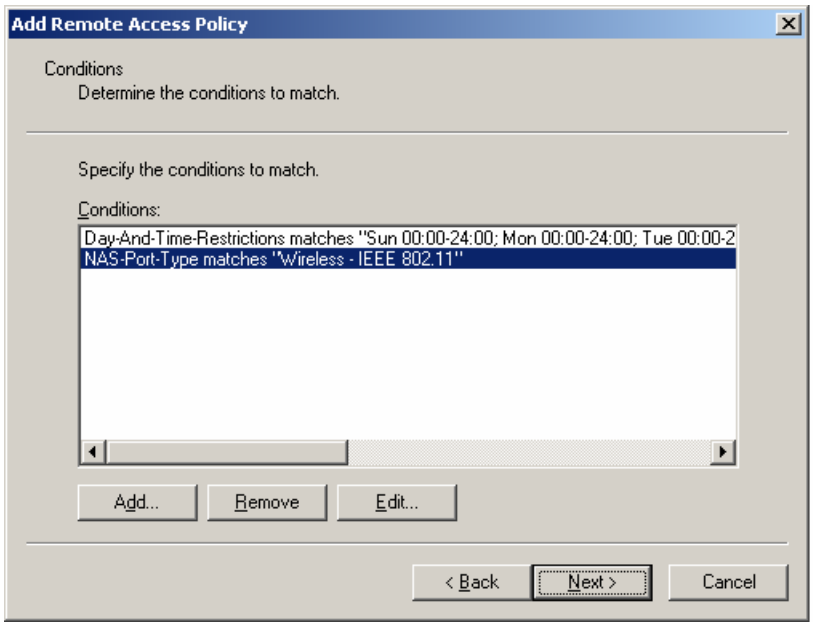
4. Select “NAS-Port-Type, the click “Add”



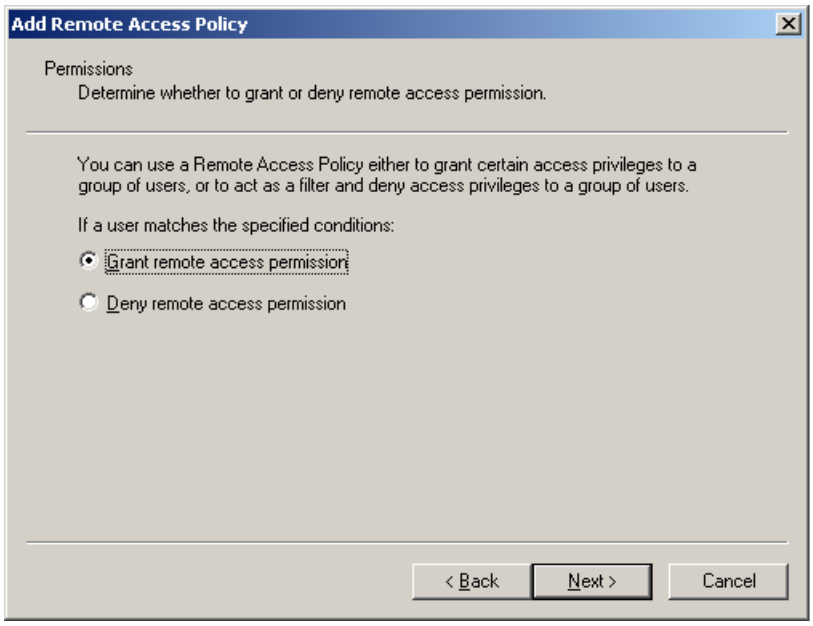
6. select “Wireless – IEEE 802.11” in the list then click the “Add” button, the click “OK”



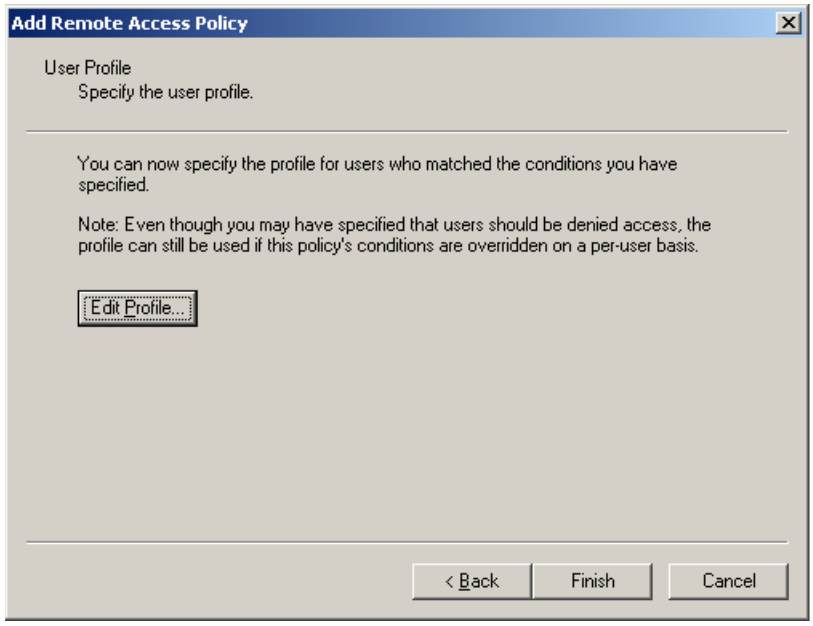
7. you should now see the NAS-Port-Type specified in the conditions list



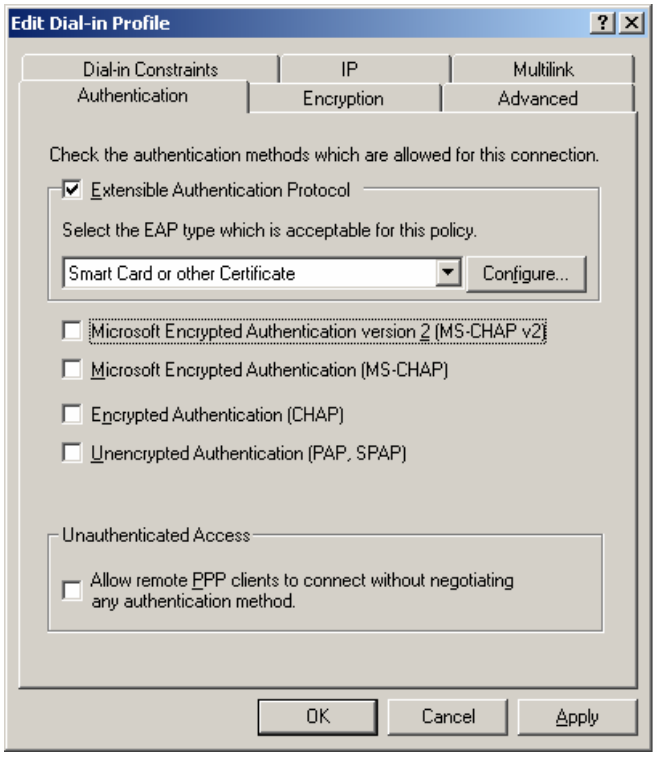
8. select “Grant remote access permission”



9. click the “Edit Profile” button

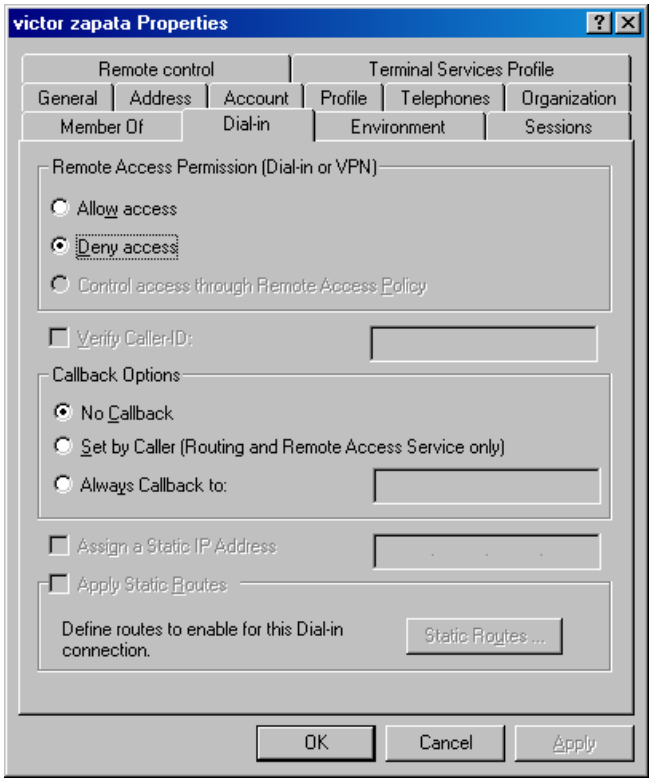


10. click on the “Authentication” tab clear all authentication methods except for “Extensible Authentication Protocol”
11. select “Smart Card or other Certificate” as the EAP type
12. click the “Configure” button and select the appropriate machine certificate

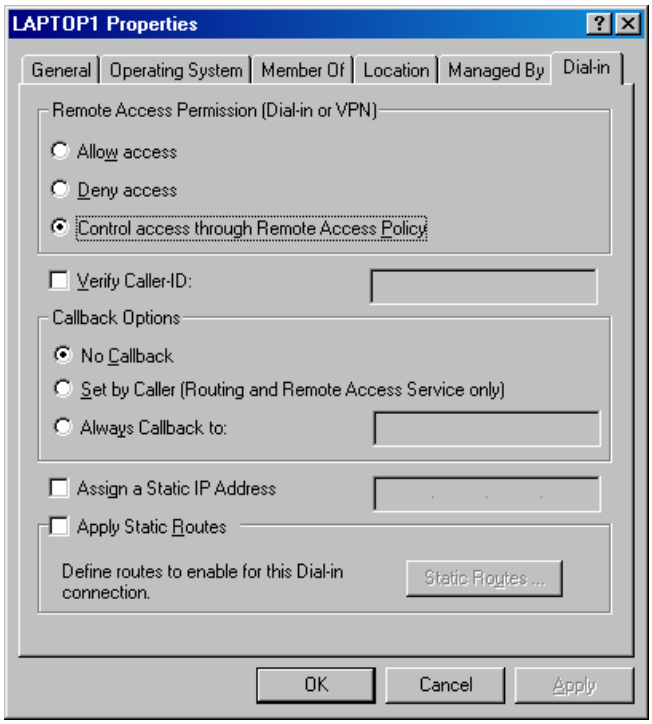


13. ensure that the “Control access through Remote Access Policy” option is enabled in the Dial-in permissions for the user account.

    * The Windows 2000 domain must be in native mode in order to enable “Control access through Remote Access Policy”



14. To configure machine authentication, ensure that the "Control access through Remote Access Policy" option is enabled in the Dial-in permissions for the machine account.



* Windows 2000 Service Pack 2 must install hotfix Q306260 in order to modify Dial-in permissions for the computer account

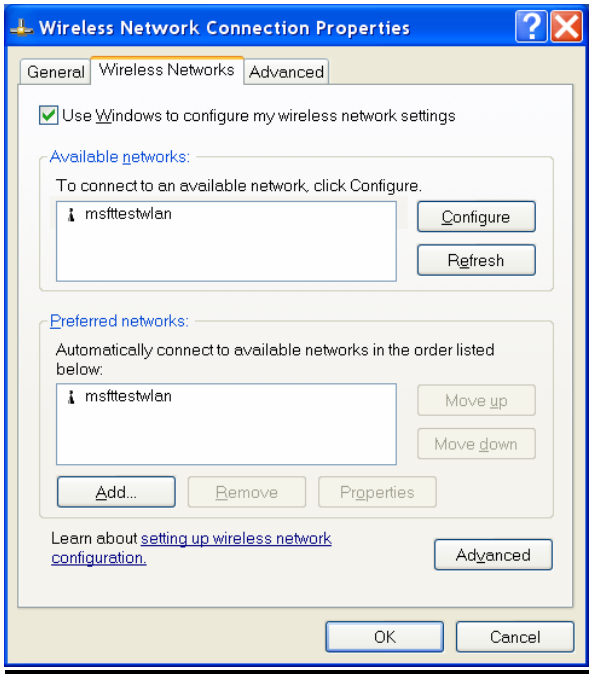
  Run the following at a command prompt after installing the hotfix:

  “ldifde -i -f %systemRoot%\system32\mac8021x.ldf -c DC=DN DC=domain,DC=com” where each "DC=" after the "DC=DN" is followed by each level of your fully qualified domain namespace (in this example the active directory domain would be domain.com).

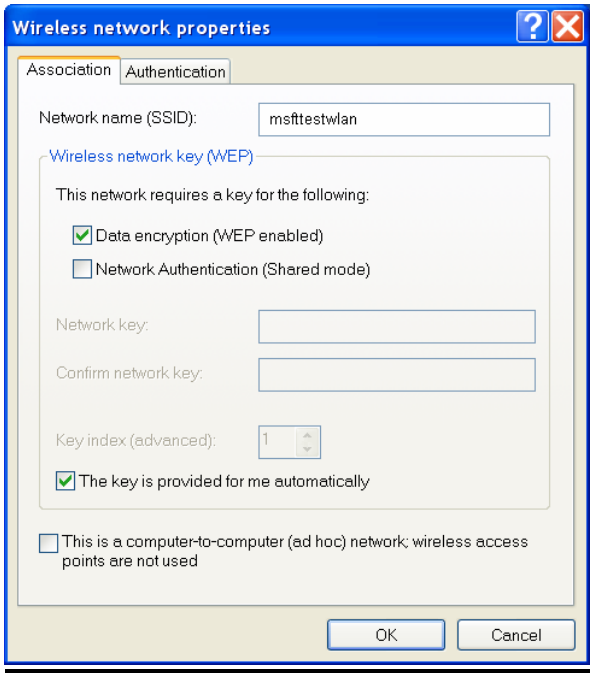
* Windows 2000 Service Pack 3 – Run the same command – No hotfix required

V. Configuring The Client for 802.1x Authentication

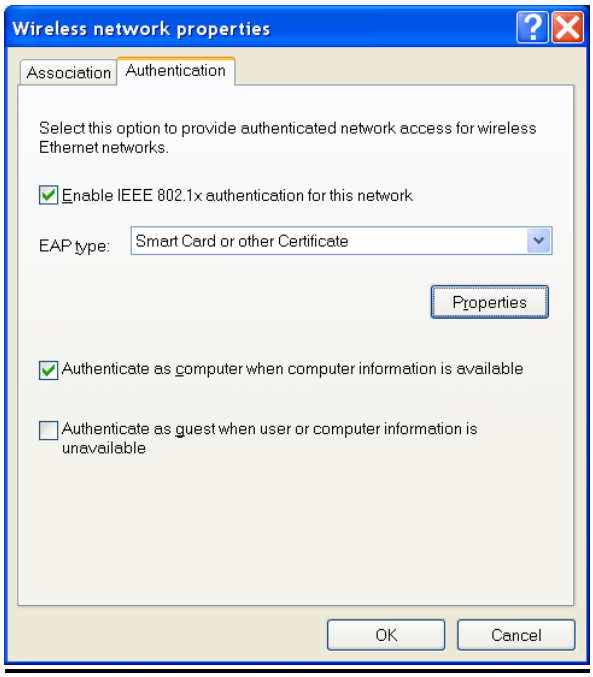
1. Open the properties of the wireless network adapter and click on the “Wireless Networks” tab
2. verify that “Use Windows to configure my wireless network settings” is enabled
3. verify that the target WLAN SSID is listed in the “Available networks” list
4. select the target WLAN from the list and click the “Configure” button



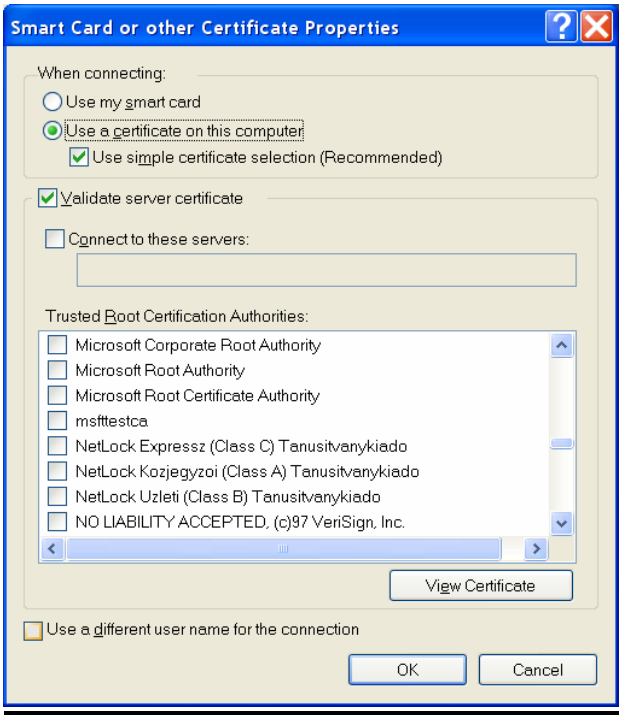
5. verify that WEP data encryption is enabled
6. verify that “The key is provided to me automatically” is enabled
7. click the “Authentication” tab



8. verify that “Enable IEEE 802.1x authentication for this network” is enabled
9. click the “Properties” button



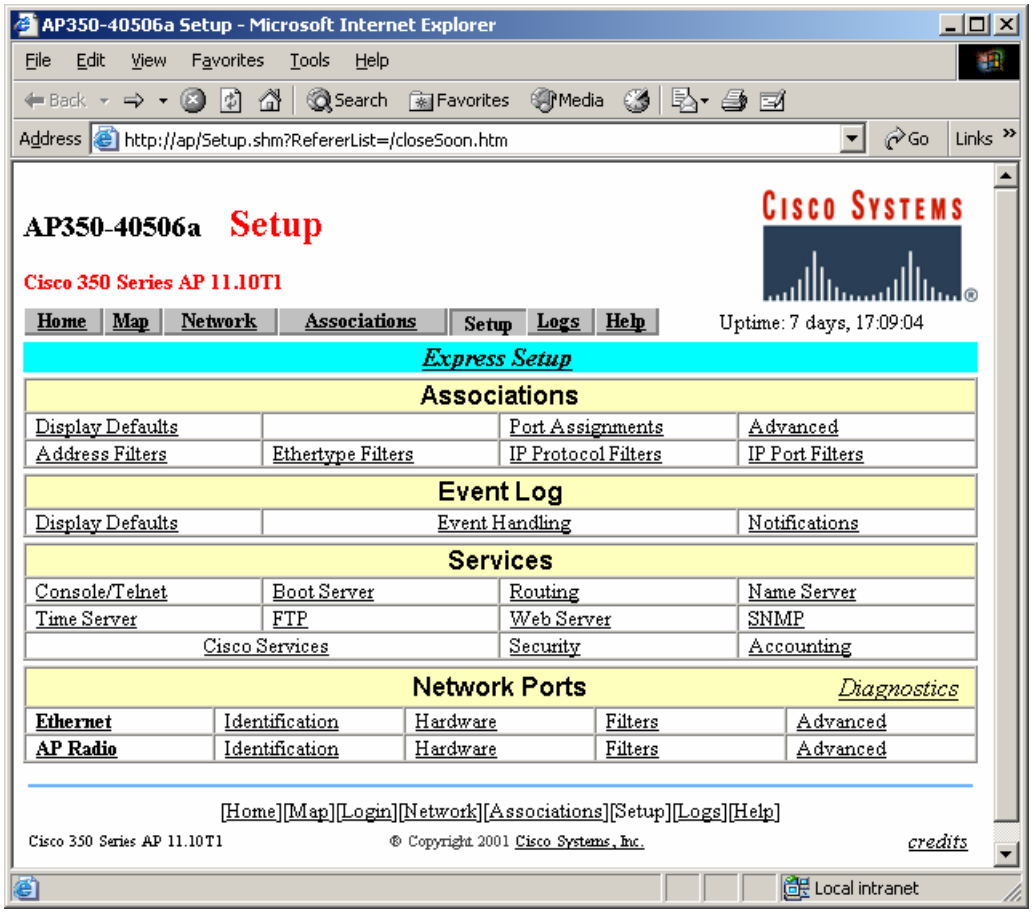
10. verify that “Use a certificate on this computer” is enabled and that “Use simple certificate selection” is checked
11. click “OK”


Smart Card or other Certificate Properties
When connecting:
Use my smart card
Use a certificate on this computer
Use simple certificate selection (Recommended)
Validate server certificate
Connect to these servers:
Trusted Root Certification Authorities:
Microsoft Corporate Root Authority
Microsoft Root Authority
Microsoft Root Certificate Authority
msfttestca
NetLock Expressz (Class C) Tanusitvanykiado
NetLock Kozjegyzoi (Class A) Tanusitvanykiado
NetLock Uzleti (Class B) Tanusitvanykiado
NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.
View Certificate
Use a different user name for the connection
OK
Cancel

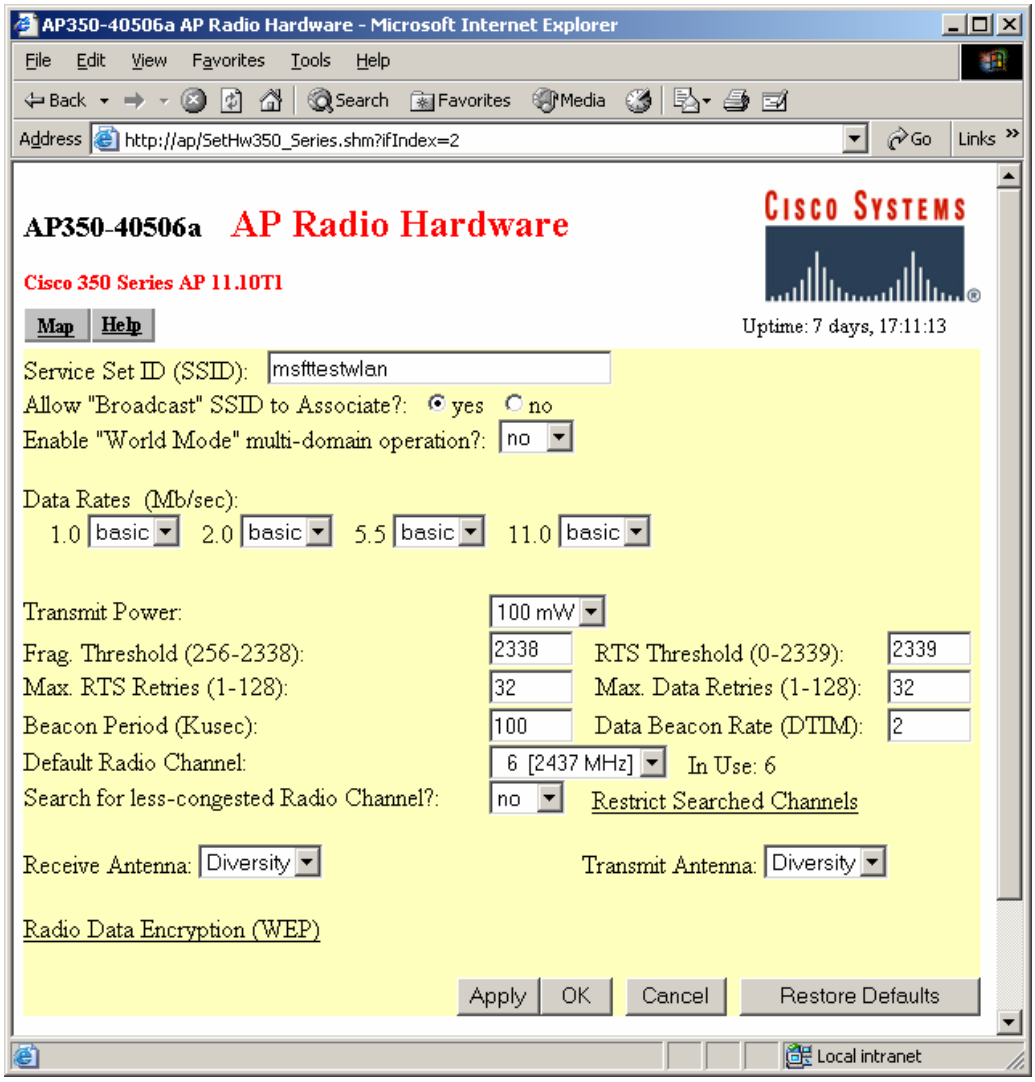
VI. Configuring The Access Point for 802.1x Authentication

a. Specify a Service Set ID (SSID) for the Access Point

1. On the AP Setup page, click on the “Identification” or “Hardware” link for the “AP Radio”

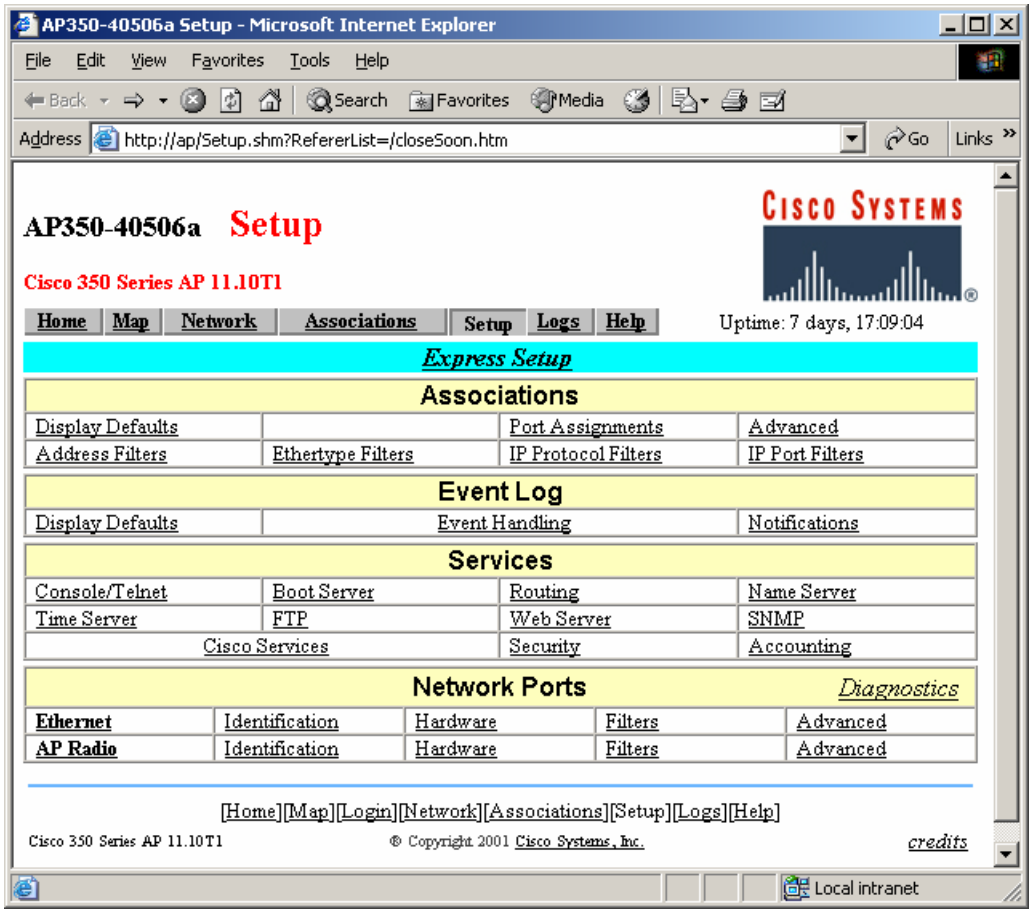


2. Enter SSID name
   a. enable/disable broadcasting of the SSID

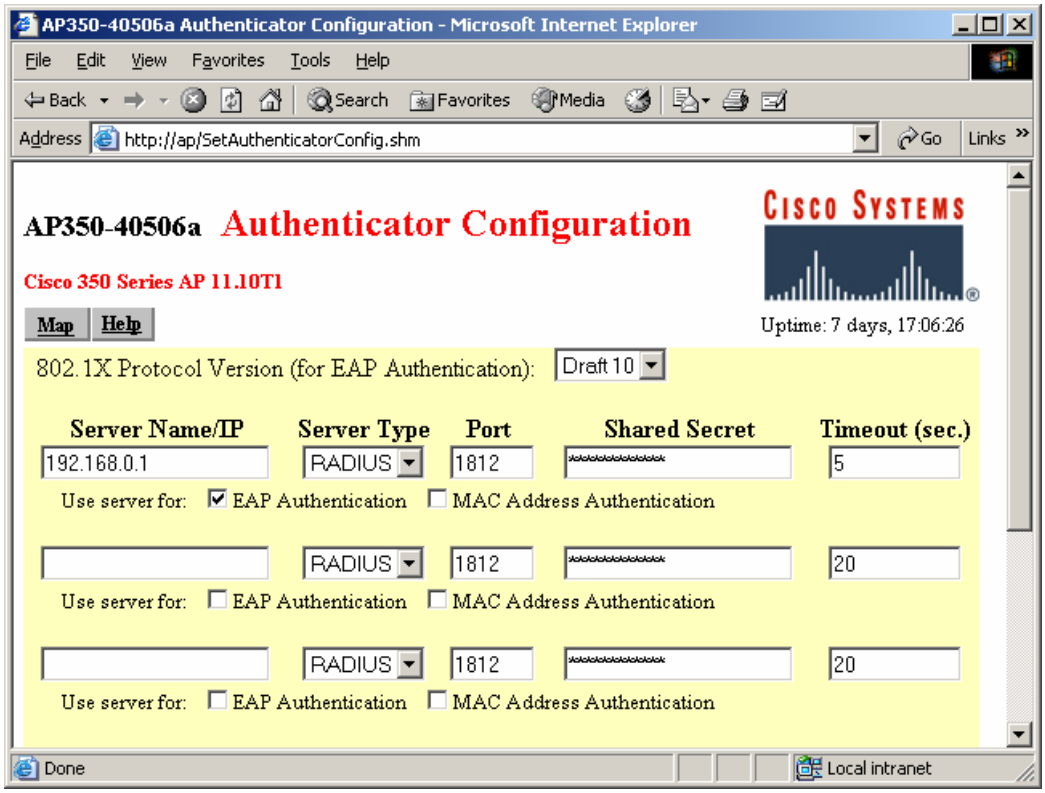


B. Configure AP for RADIUS authentication

1. click on the “Security” link from the AP Setup page

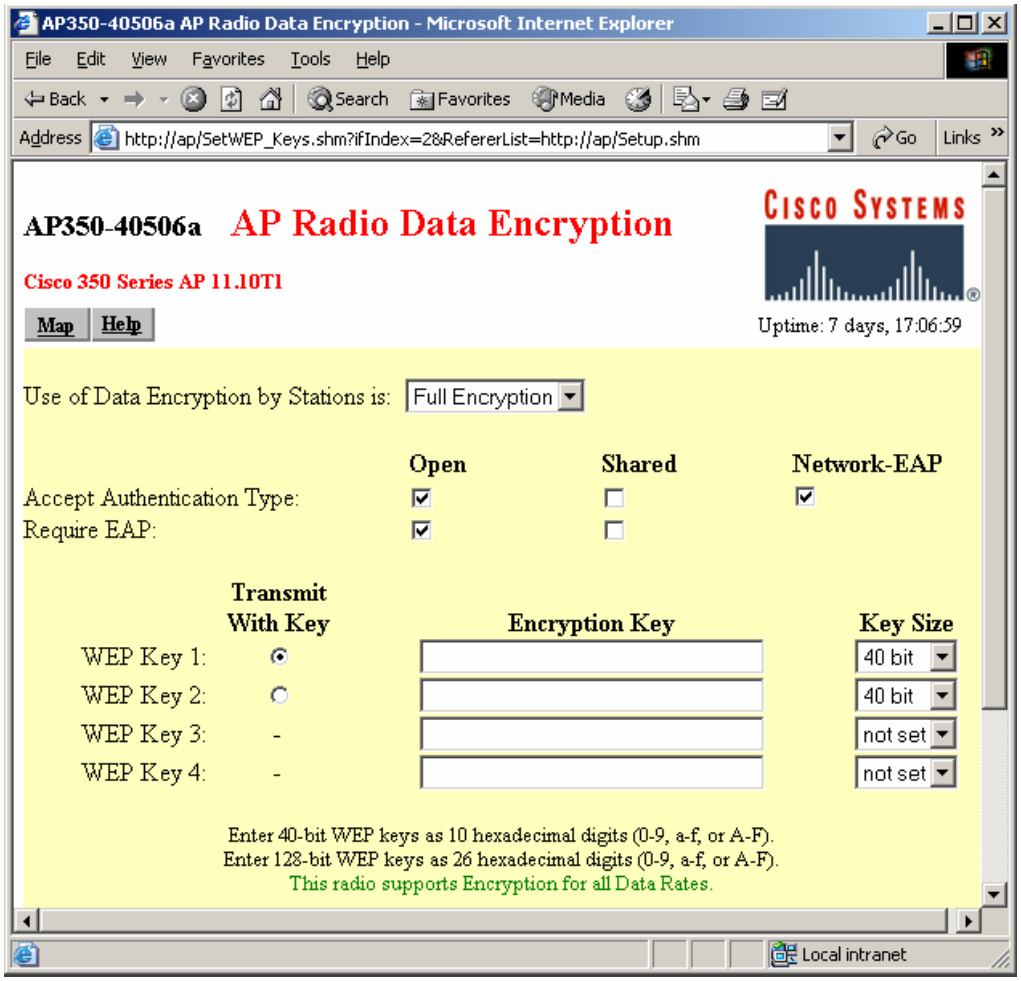


2. enter the name or IP address of the Windows 2000 IAS server.
3. select “RADIUS” as the Server Type
4. enter shared secret previously specified on the Windows 2000 IAS server



C. Configure AP Data Encryption using Wired Equivalent Privacy (WEP)

1. select “Full Encryption” for Data Encryption
2. enable the “Open” and “Network-EAP” options for “Accept Authentication Type”
3. enable the “Open” option for “Require EAP”
4. create WEP key/s
   a. NOTE: to utilize WEP key rotation, you must create multiple WEP keys


AP350-40506a AP Radio Data Encryption - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://ap/SetWEP_Keys.shm?ifIndex=2&RefererList=http://ap/Setup.shm
Go Links
AP350-40506a AP Radio Data Encryption
Cisco 350 Series AP 11.10T1
Map Help
Cisco Systems
Uptime: 7 days, 17:06:59
Use of Data Encryption by Stations is: Full Encryption
Open Shared Network-EAP
Accept Authentication Type:
Require EAP:
Transmit With Key
Encryption Key
Key Size
WEP Key 1: 40 bit
WEP Key 2: 40 bit
WEP Key 3: - not set
WEP Key 4: - not set
Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).
Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F).
This radio supports Encryption for all Data Rates.
Local intranet

v.1.1