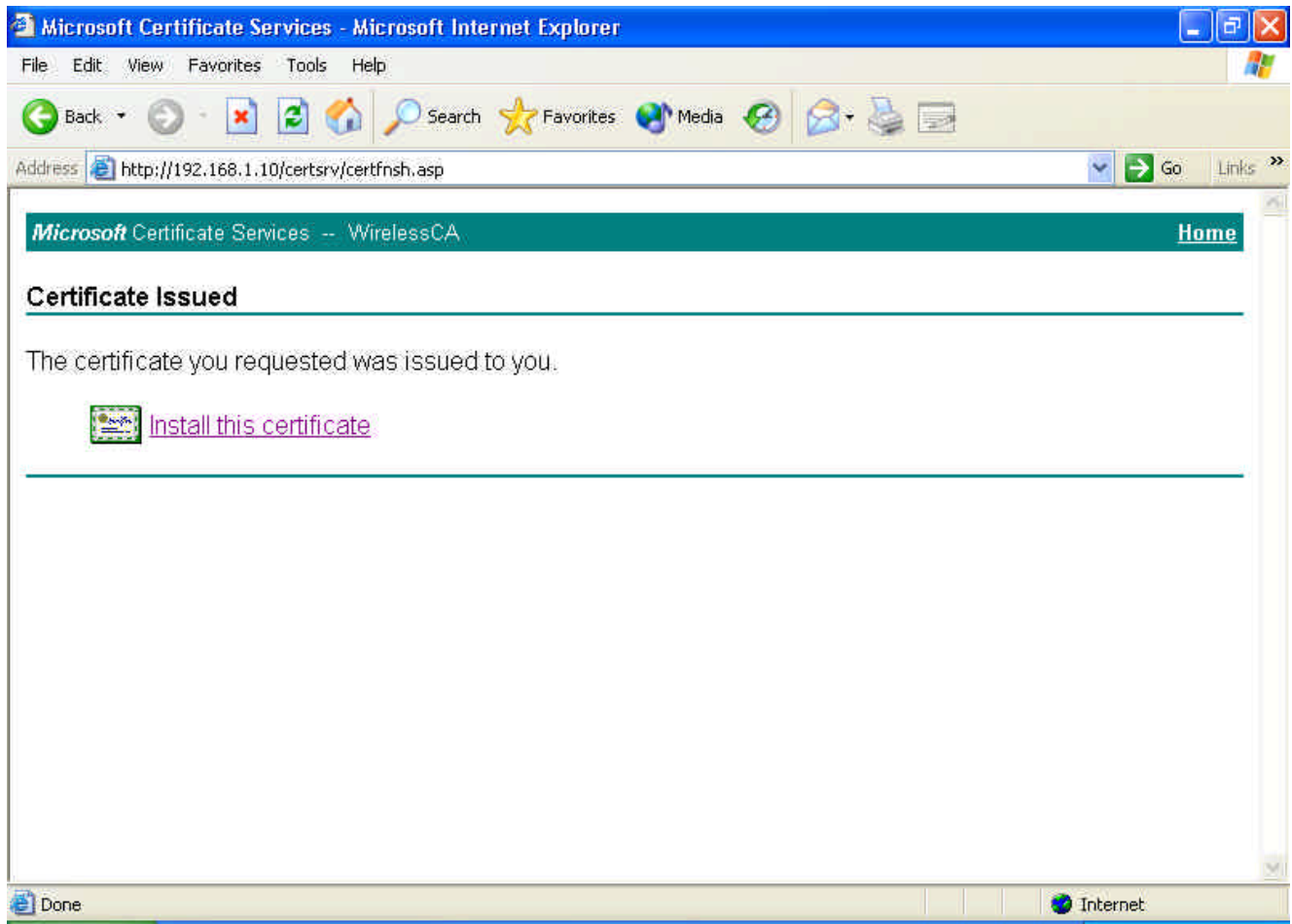
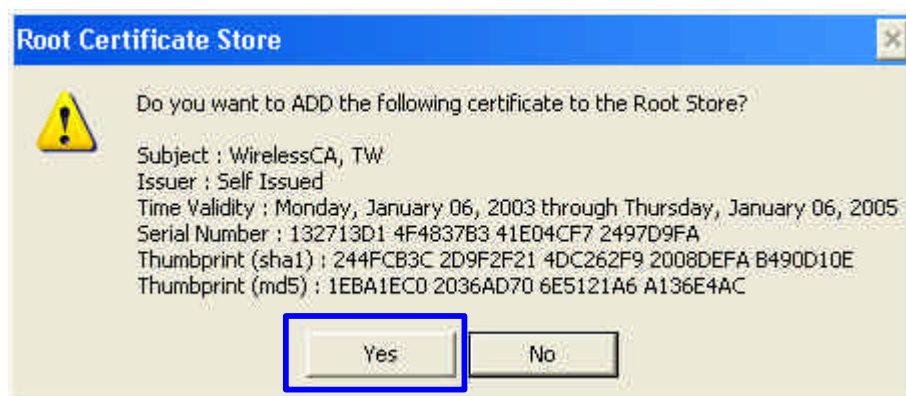


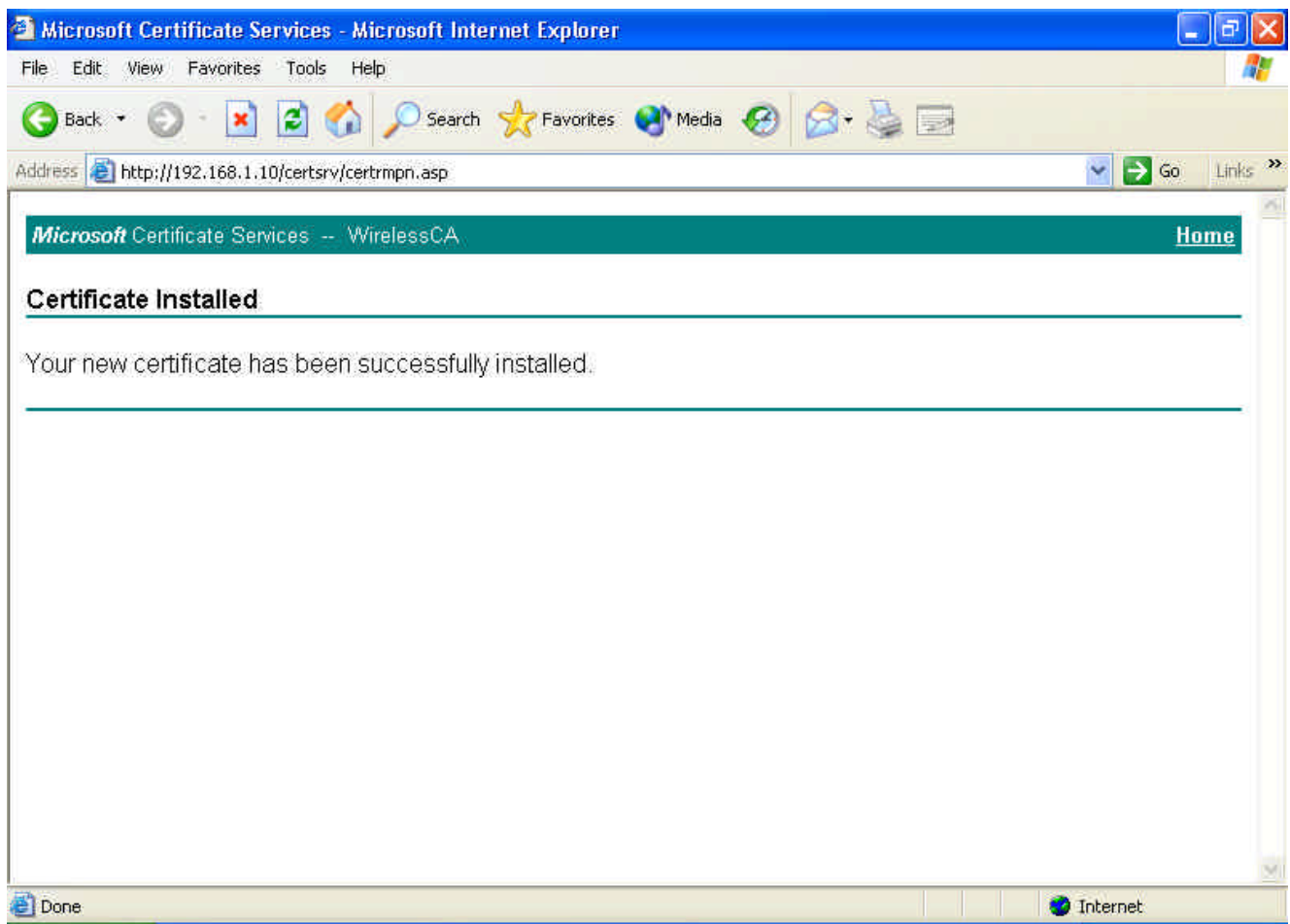
20. The certificate is issued by the server, click “Install this certificate” to download and store the certificate to your local computer.



21. Click “Yes” to store the certificate to your local computer.

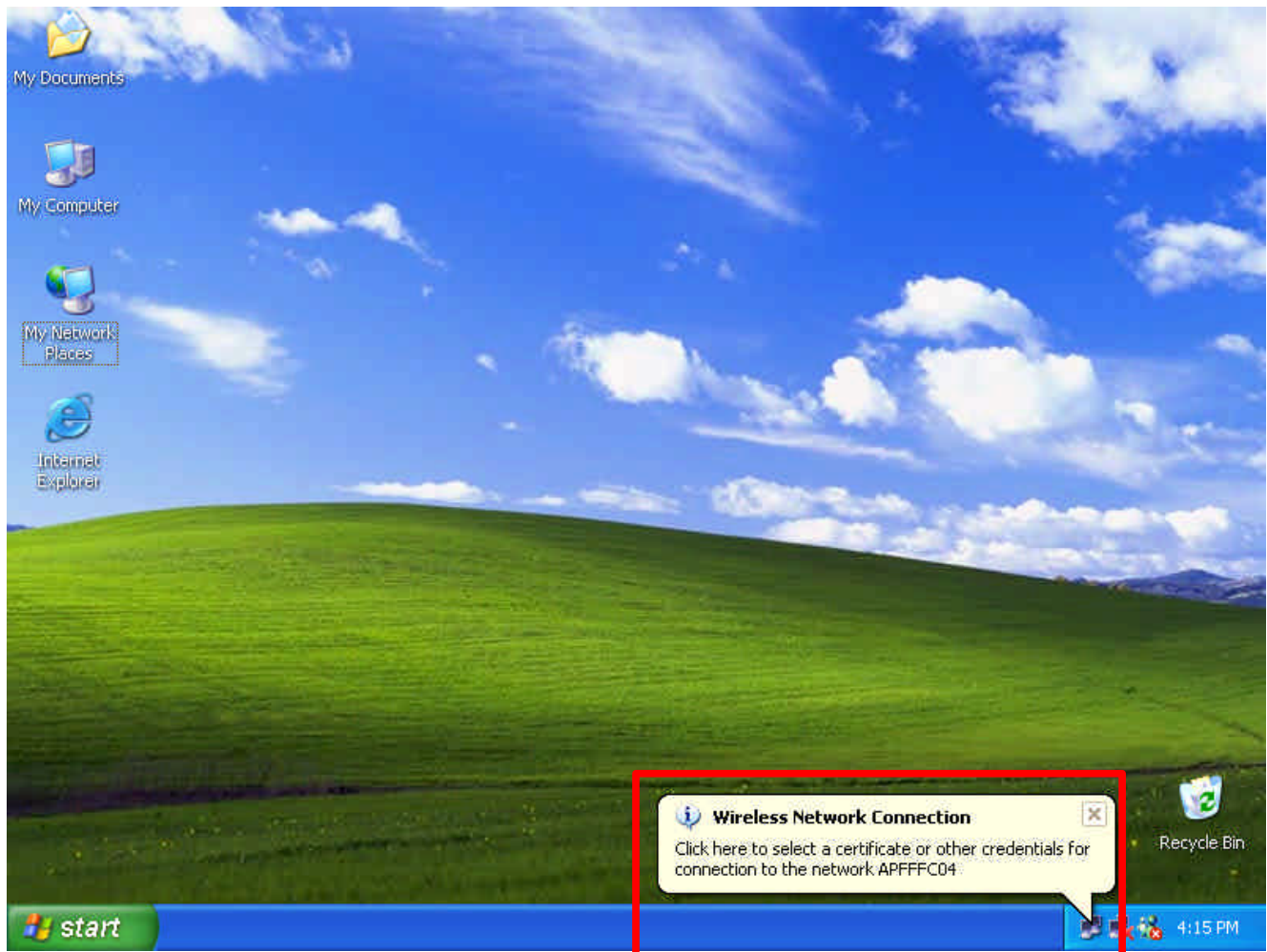


22. Certificate is now installed.

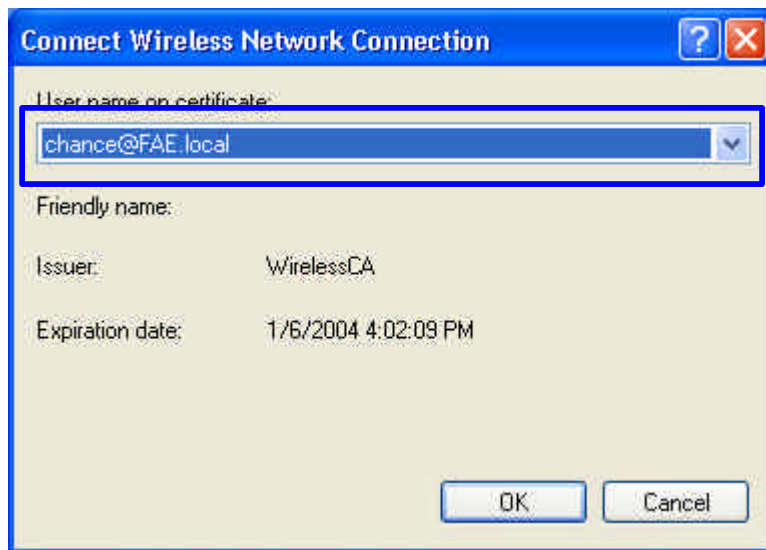


All the configuration and certificate download are now complete. Let's try to connect to the Access Point using 802.1x TLS Authentication.

23. Windows XP will prompt you to select a certificate for wireless network connection. Click on the network connection icon in the system tray to continue.



24. Select the certificate that was issued by the server (WirelessCA), and click “OK” to continue.

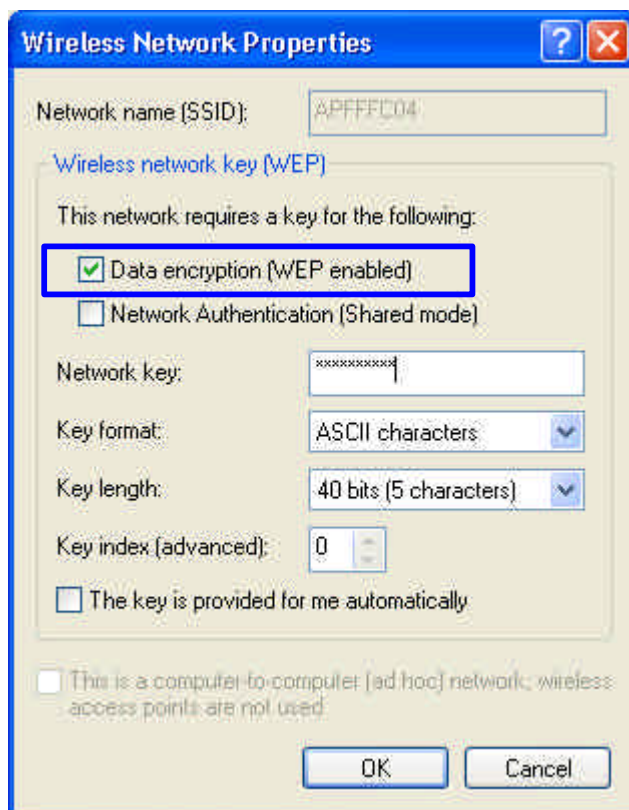


25. Check the server to make sure that it's the server that issues certificate, and click “OK” to complete the authentication process.



MD5 Authentication

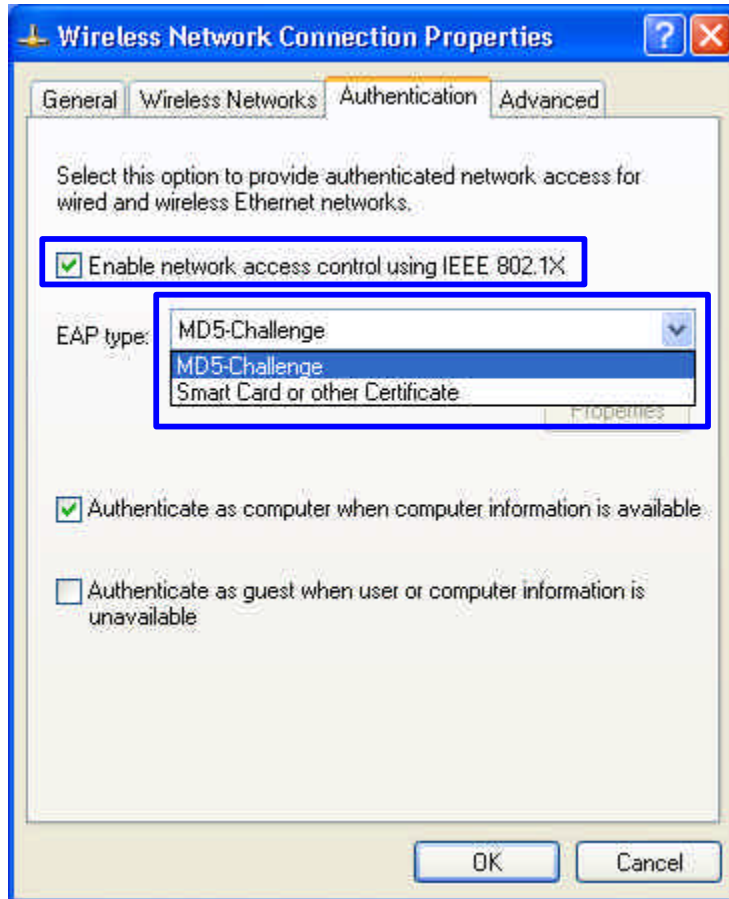
26. Select “**Data encryption (WEP enabled)**” option, but leave other option unselected.
27. Select the **key format** that you want to use to key in your Network key.
 ASCII characters: 0~9, a~z and A~Z
 HEX characters: 0~9, a~f
28. Select the **key length** that you wish to use
 40 bits (5 characters for ASCII, 10 characters for HEX)
 104 bits (13 characters for ASCII, 26 characters for HEX)
29. After deciding the key format and key length that you wish to use for network key. Enter the network key in “**Network key**” text box.



Please note that that value of Network key entered, and key format/length used, must be the same as that used in the Access Point. Although there are 4 set of keys can be set in the Access Point WEP configuration, it's the **first set** of key that must be the same as that we used by the supplicant wireless client.

30. Click “**OK**” to close the Wireless Network Properties window, thus make the changes effective.

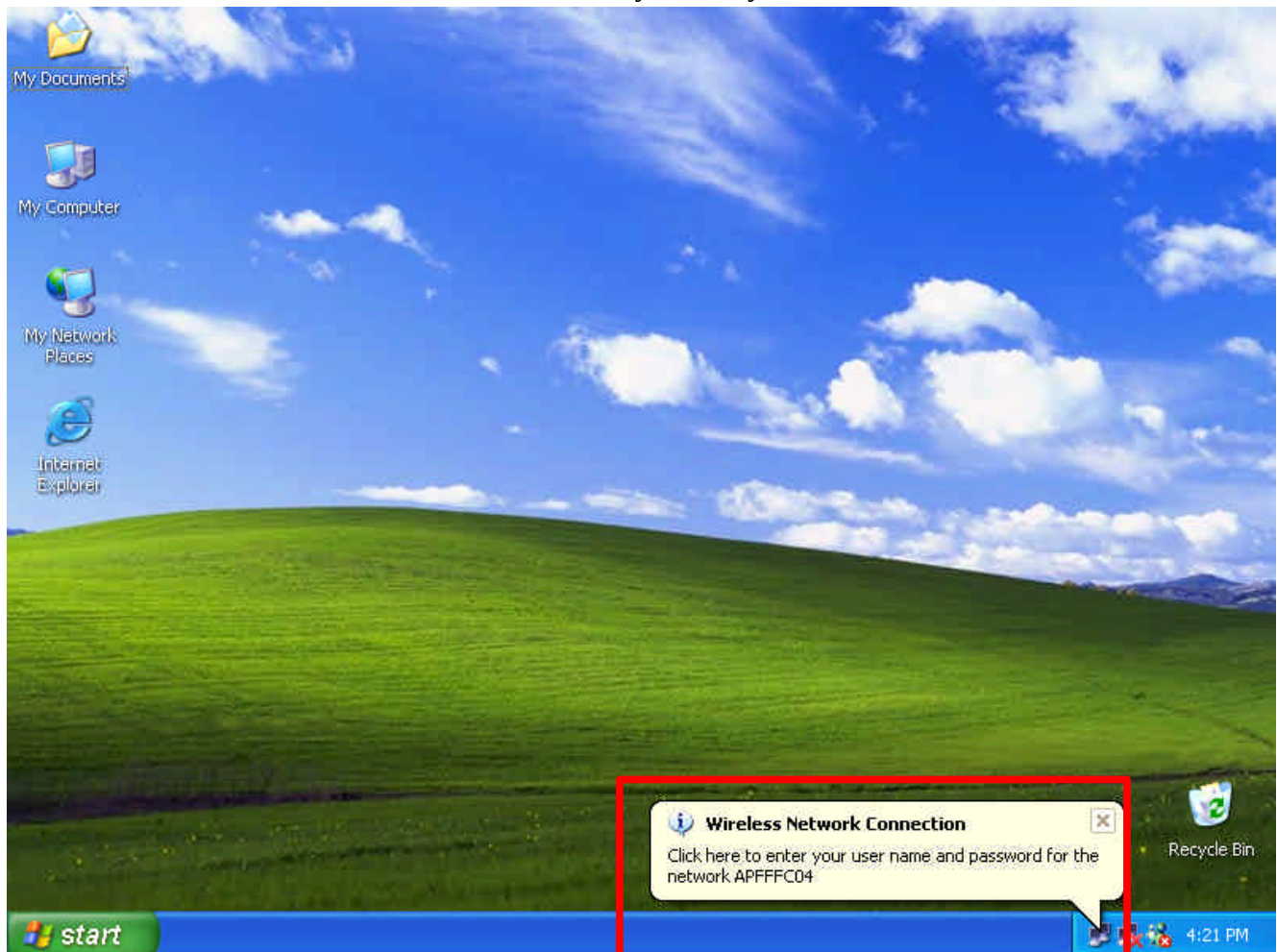
31. Select “**Authentication**” tab.
32. Select “**Enable network access control using IEEE 802.1X**” to enable 802.1x authentication.
33. Select “**MD-5 Challenge**” from the drop-down list box for EAP type.



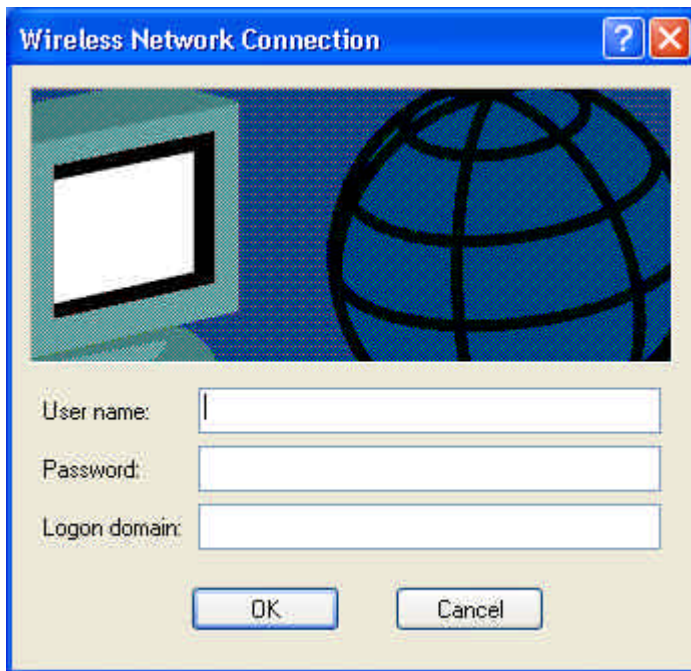
34. Click “**OK**” to close Wireless Network Connection Properties window, thus make all the changes effective.

Unlike TLS, which uses digital certificate for validation, the MD-5 Authentication is based on the user account/password. Therefore, you must have a valid account used by the server for validation.

35. WindowsXP will prompt you to enter your user name and password. Click on the network connection icon in the system tray to continue.



36. Enter the user name, password and the logon domain that your account belongs if you have one or more network domain exist in your network.
37. Click “**OK**” to complete the validation process.



Authenticator: Wireless Network Access Point

This is the web page configuration in the Access Point that we use.

The screenshot shows the configuration page for an Access Point. The top navigation bar includes links for 'wizard', 'Status', 'Basic Setting', 'IP Setting', 'Advanced Setting', 'Security', '802.1x', and 'Tools'. The '802.1x' tab is selected. The main content area is titled '802.1x' and contains the following settings:

- 802.1x** ☒ Enabled ☐ Disabled
- Encryption Key Length** ☒ 64 bits ☐ 128 bits ☐ 256bits
- Lifetime** 30 Minutes (dropdown menu)
- RADIUS Server 1**
 - IP**: [0] [.] [0] [.] [0] [.] [0]
 - Port**: 1812
 - Shared Secret**: [text input field]
- RADIUS Server 2 (optional)**
 - IP**: [0] [.] [0] [.] [0] [.] [0]
 - Port**: [0]
 - Shared Secret**: [text input field]

At the bottom, there are three buttons: 'Apply', 'Cancel', and 'Help'.

1. Enable 802.1x security by selecting “**Enable**”.
2. If **MD5** EAP methods is used then you can skip step 3 and go to step 4.
3. Select the **Encryption Key Length Size** ranging from 64 to 256 Bits that you would like to use.
Select the **Lifetime of the Encryption Key** from 5 Minutes to 1 Day. As soon as the lifetime of the Encryption Key is over, the Encryption Key will be renewed by the Radius server.
4. Enter the **IP address** of and the **Port** used by the **Primary** Radius Server
Enter the **Shared Secret**, which is used by the Radius Server.
5. Enter the **IP address** of, **Port** and **Shared Secret** used by the **Secondary** Radius Server.
6. Click “**Apply**” button for the 802.1x settings to take effect after Access Point reboots itself.

Note!: As soon as 802.1x security is enabled, all the wireless client stations that are connected to the Access Point currently will be disconnected. The wireless clients must be configured manually to authenticate themselves with the Radius server to be reconnected.

Radius Server: Window2000 Server

This section to help those who has Windows 2000 Server installed and wants to setup Windows2000 Server for 802.1x authentication, which includes setting up Certificate Service for TLS Authentication, and enable EAP-methods.

1. Login into your Windows 2000 Server as Administrator, or account that has Administrator authority.
2. Go to **Start > Control Panel**, and double-click “Add or Remove Programs”
3. Click on “**Add/Remove Windows components**”
4. Check “**Certificate Services**”, and click “Next” to continue.



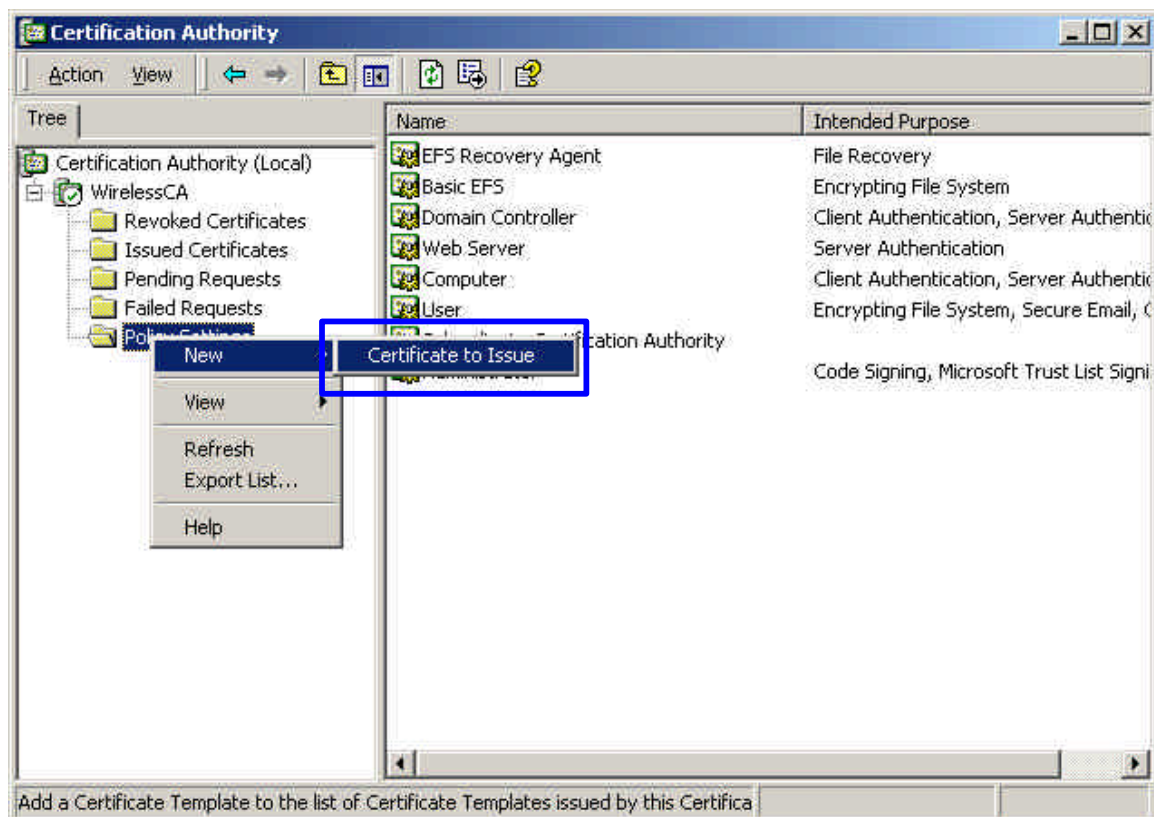
5. Select “**Enterprise root CA**”, and click “**Next**” to continue.

The screenshot shows the 'Windows Components Wizard' window. The title bar is blue with the text 'Windows Components Wizard'. The main window has a white header area with the title 'Certification Authority Type' and a subtitle 'There are four types of certification authorities.' Below this, there are two columns. The left column is titled 'Certification Authority types:' and contains four radio button options: 'Enterprise root CA' (which is selected), 'Enterprise subordinate CA', 'Stand-alone root CA', and 'Stand-alone subordinate CA'. The right column is titled 'Description:' and contains a text box with the text: 'The most trusted CA in an enterprise. Should be installed before any other CA. Requires Active Directory.' At the bottom left, there is a checkbox labeled 'Advanced options' which is unchecked. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

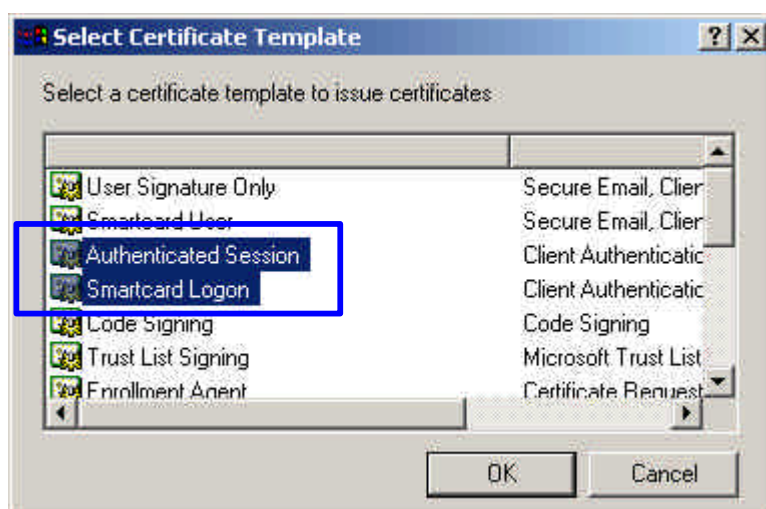
6. Enter the information that you want for your Certificate Service, and click “**Next**” to continue.

The screenshot shows the 'Windows Components Wizard' window. The title bar is blue with the text 'Windows Components Wizard'. The main window has a white header area with the title 'CA Identifying Information' and a subtitle 'Enter information to identify this CA'. Below this, there are several input fields. The first field is 'CA name:' with the text 'WirelessCA' entered. Below it are 'Organization:', 'Organizational unit:', 'City:', 'State or province:', and 'E-mail:' fields, all of which are empty. To the right of the 'State or province:' field is a 'Country/region:' field with the text 'US' entered. Below these fields is a 'CA description:' field, which is empty. At the bottom left, there is a 'Valid for:' field with the text '2' entered in a box, followed by a dropdown menu showing 'Years'. To the right of this is an 'Expires:' field with the text '1/8/2005 12:15 PM' entered. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

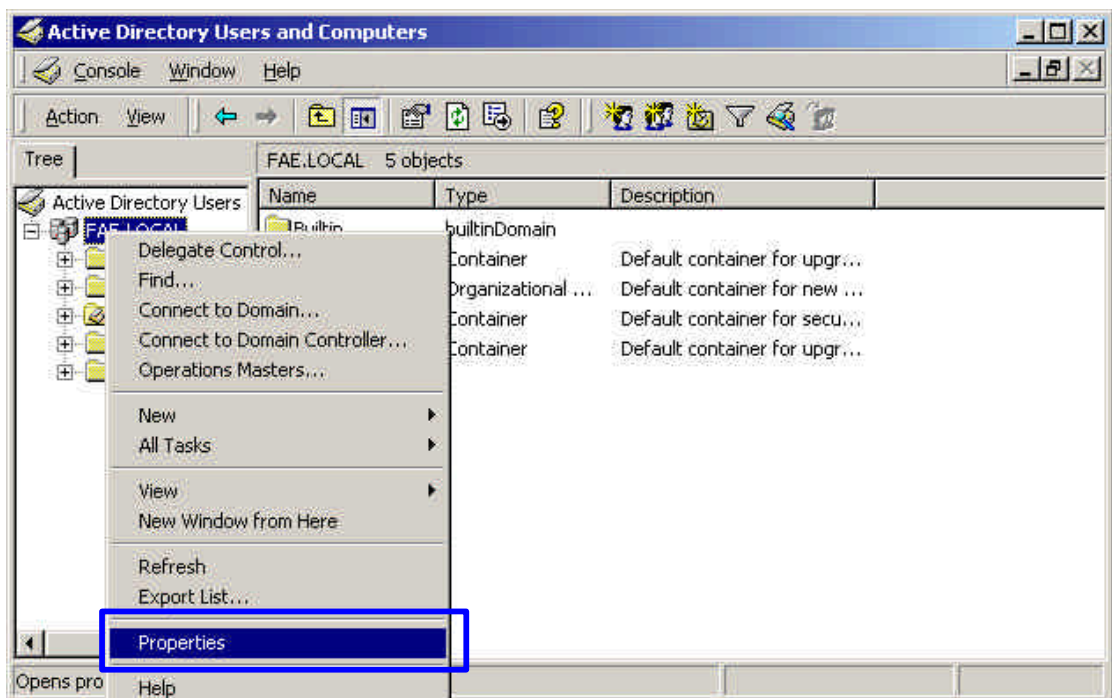
7. Go to Start > Program > Administrative Tools > **Certificate Authority**
8. Right-click on the “**Policy Setting**”, select “**new**”
9. Select “**Certificate to Issue**”



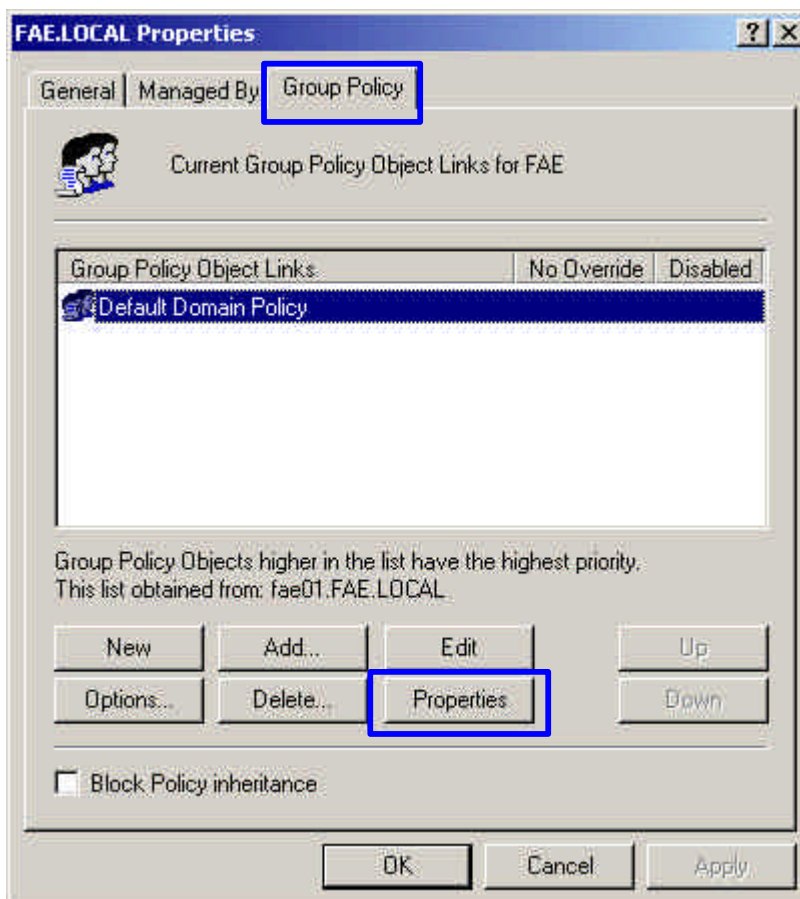
10. Select “**Authenticated Session**” and “**Smartcard Logon**” by holding down to the Ctrl key, and click “**OK**” to continue.



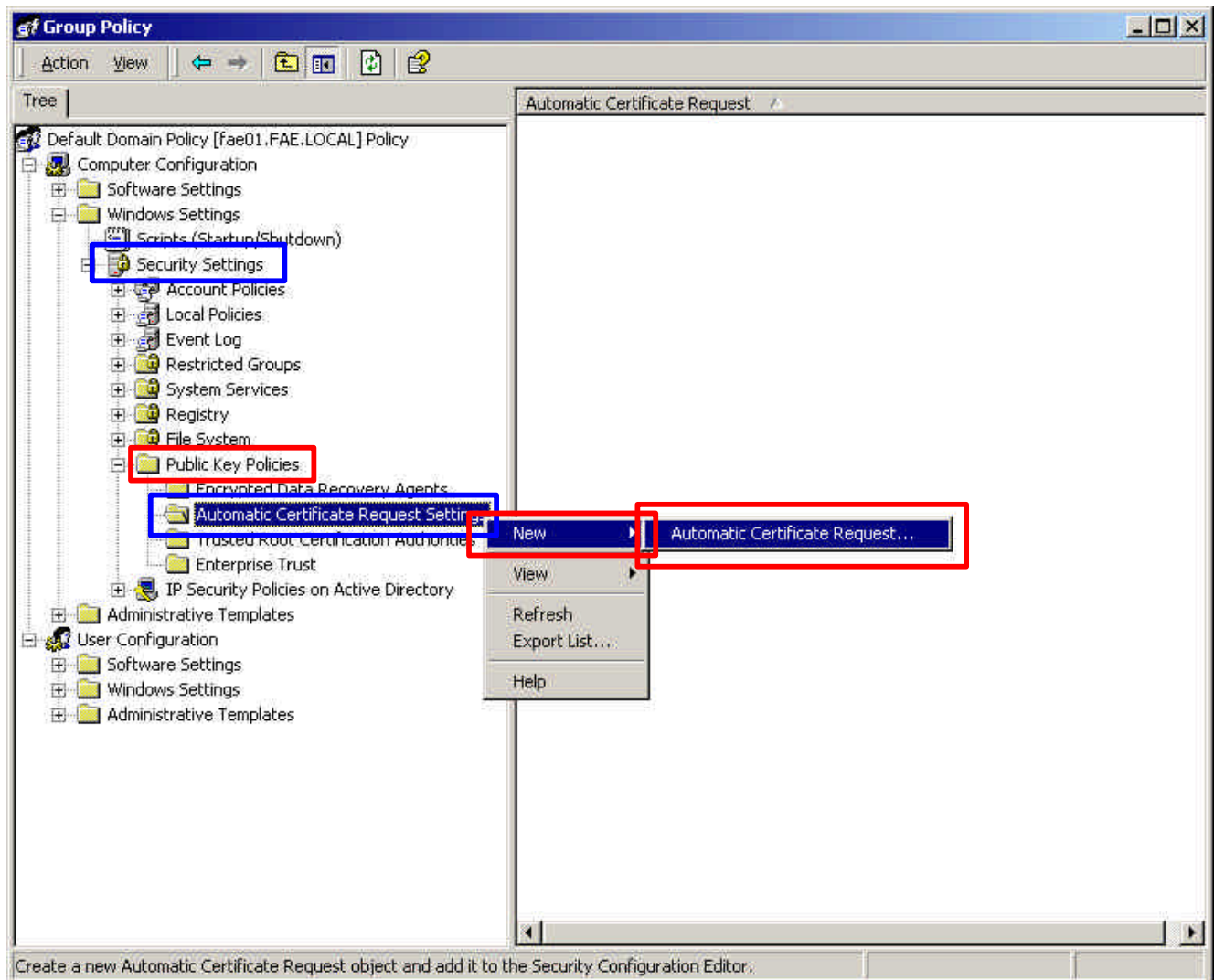
11. Go to Start > Program > Administrative Tools > **Active Directory Users and Computers**.
12. Right-click on domain, and select "**Properties**" to continue.



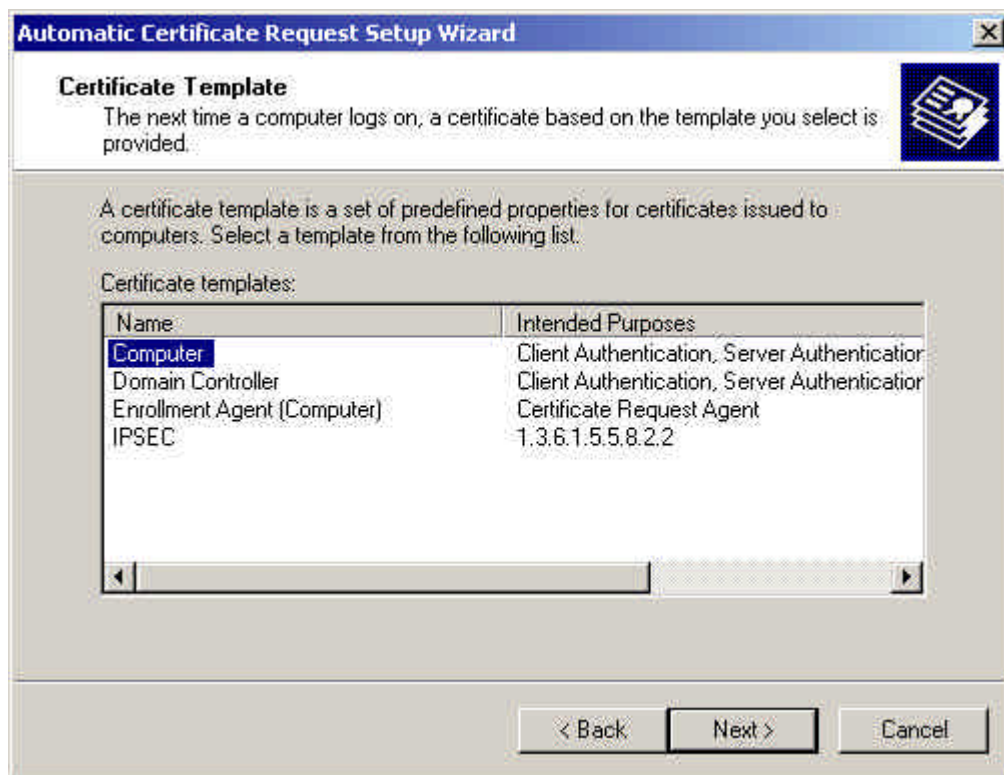
13. Select "**Group Policy**" tab and click "**Properties**" to continue.



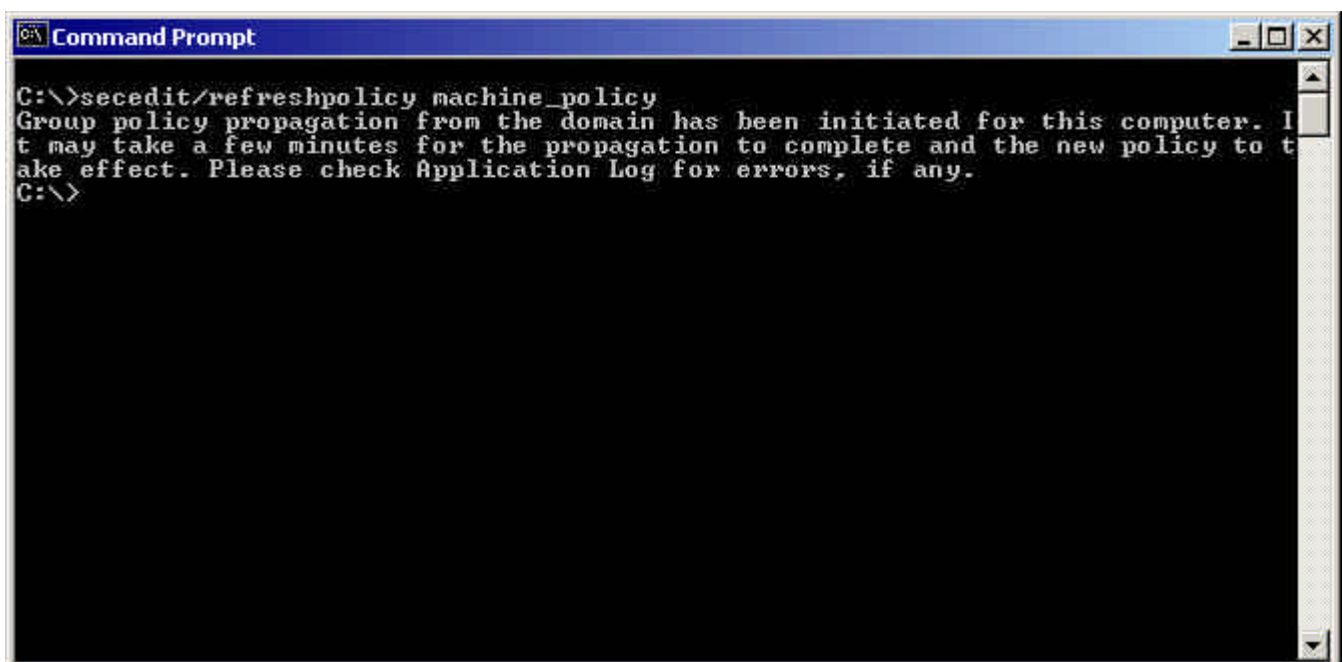
14. Go to “Computer Configuration” > “Security Settings” > **“Public Key Policies”**
15. Right-click **“Automatic Certificate Request Setting”**, and select **“New”**
16. Click **“Automatic Certificate Request ...”**



17. The Automatic Certificate Request Setup Wizard will guide you through the Automatic Certificate Request setup, simply click “**Next**” through to the last step.

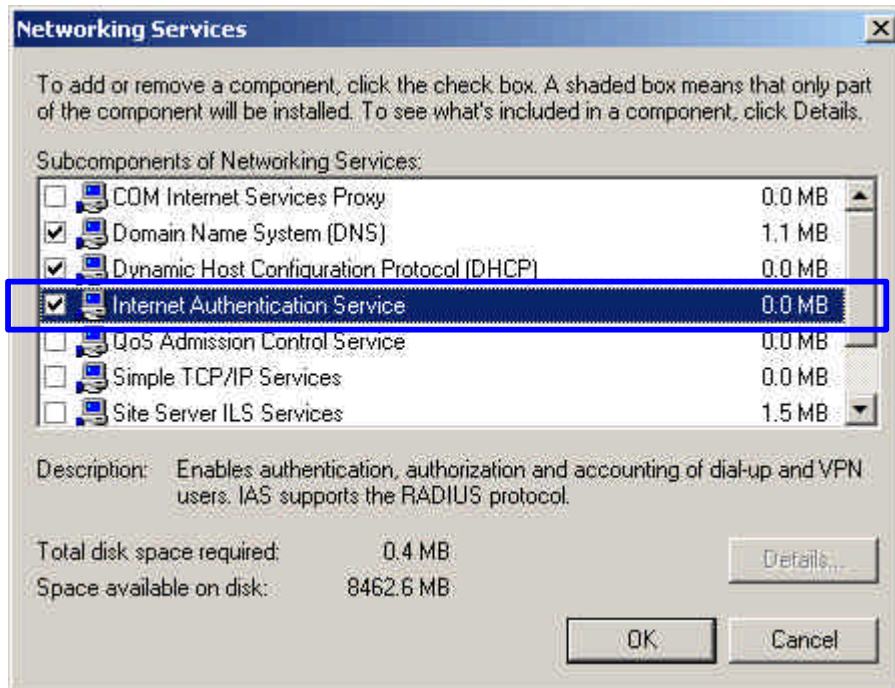


18. Click “**Finish**” to complete the Automatic Certificate Request Setup
19. Go to Start > **Run**, and type “**command**” and click “**Enter**” to open Command Prompt.
20. Type “secedit/refreshpolicy machine_policy” to refresh policy.



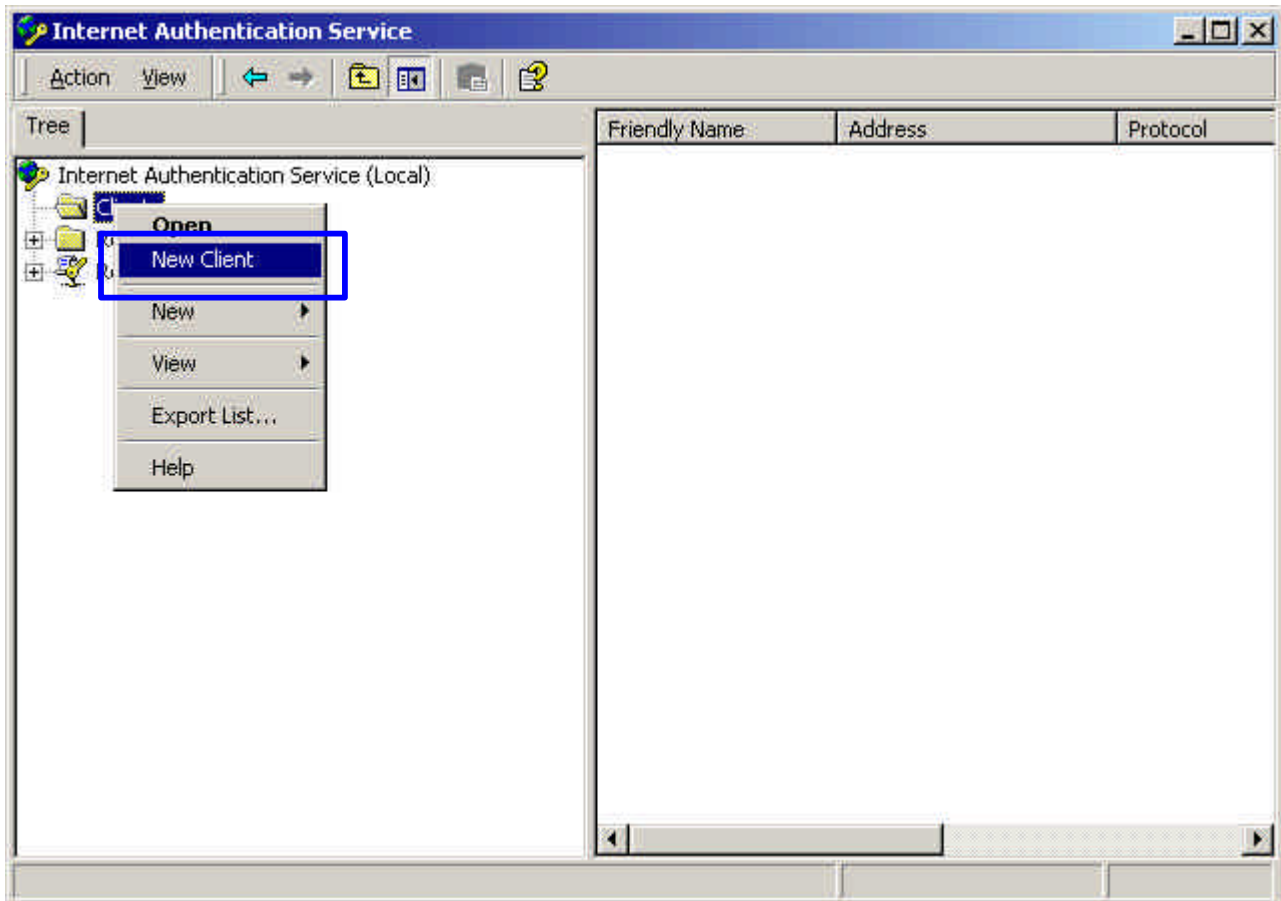
Adding Internet Authentication Service

21. Go to Start > Control Panel > **Add or Remove Programs**
22. Select “**Add/Remove Windows Components**” from the panel on the left.
23. Select “**Internet Authentication Service**”, and click “**OK**” to install.

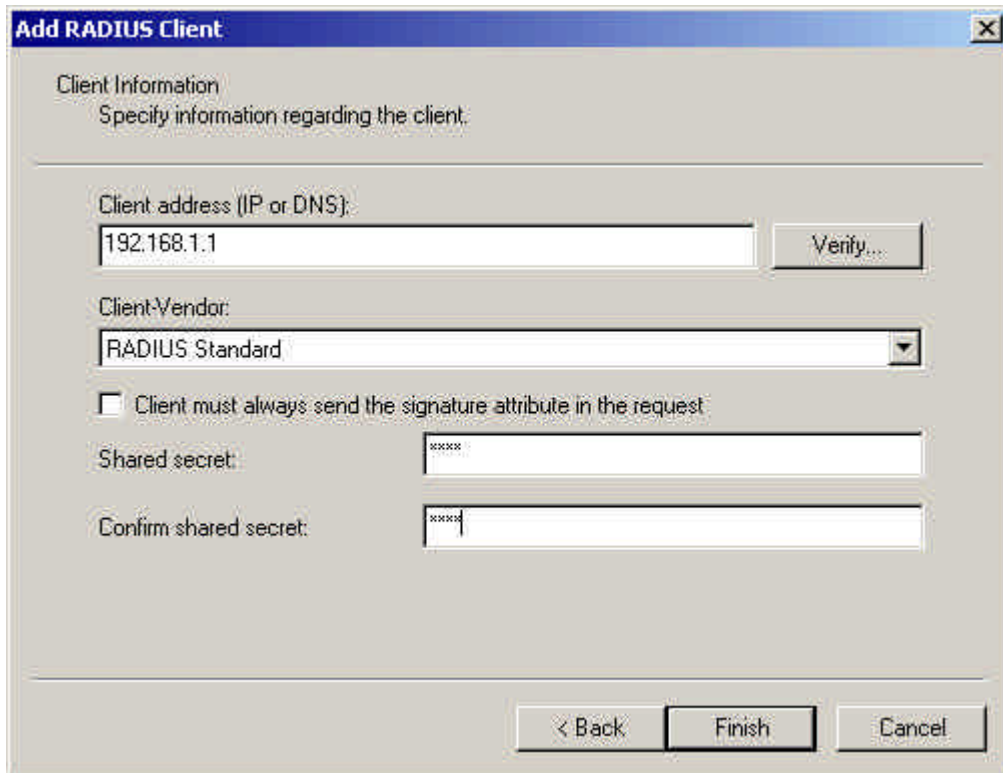


Setting Internet Authentication Service

24. Go to Start > Program > Administrative Tools > **Internet Authentication Service**
25. Right-click “**Client**”, and select “**New Client**”



26. Enter the IP address of the Access Point in the **Client address** text field, a memorable name for the Access Point in the **Client-Vendor** text field, the access password used by the Access Point in the **Shared secret** text field. Re-type the password in the **Confirmed shared secret** text field.
27. Click “Finish” to complete adding of the Access Point.



The image shows a Windows-style dialog box titled "Add 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 "Client Information" is followed by the instruction "Specify information regarding the client:". The main area of the dialog contains several input fields and a checkbox. The first field is labeled "Client address (IP or DNS):" and contains the text "192.168.1.1". To the right of this field is a button labeled "Verify...". Below this is a field labeled "Client-Vendor:" which is a dropdown menu currently showing "RADIUS Standard". Below the dropdown is a checkbox with the label "Client must always send the signature attribute in the request". Below the checkbox are two more fields: "Shared secret:" and "Confirm shared secret:". Both of these fields contain masked text represented by "x" characters. At the bottom of the dialog, there are three buttons: "< Back", "Finish", and "Cancel".

Add RADIUS Client

Client Information
Specify information regarding the client.

Client address (IP or DNS):
192.168.1.1 Verify...

Client-Vendor:
RADIUS Standard

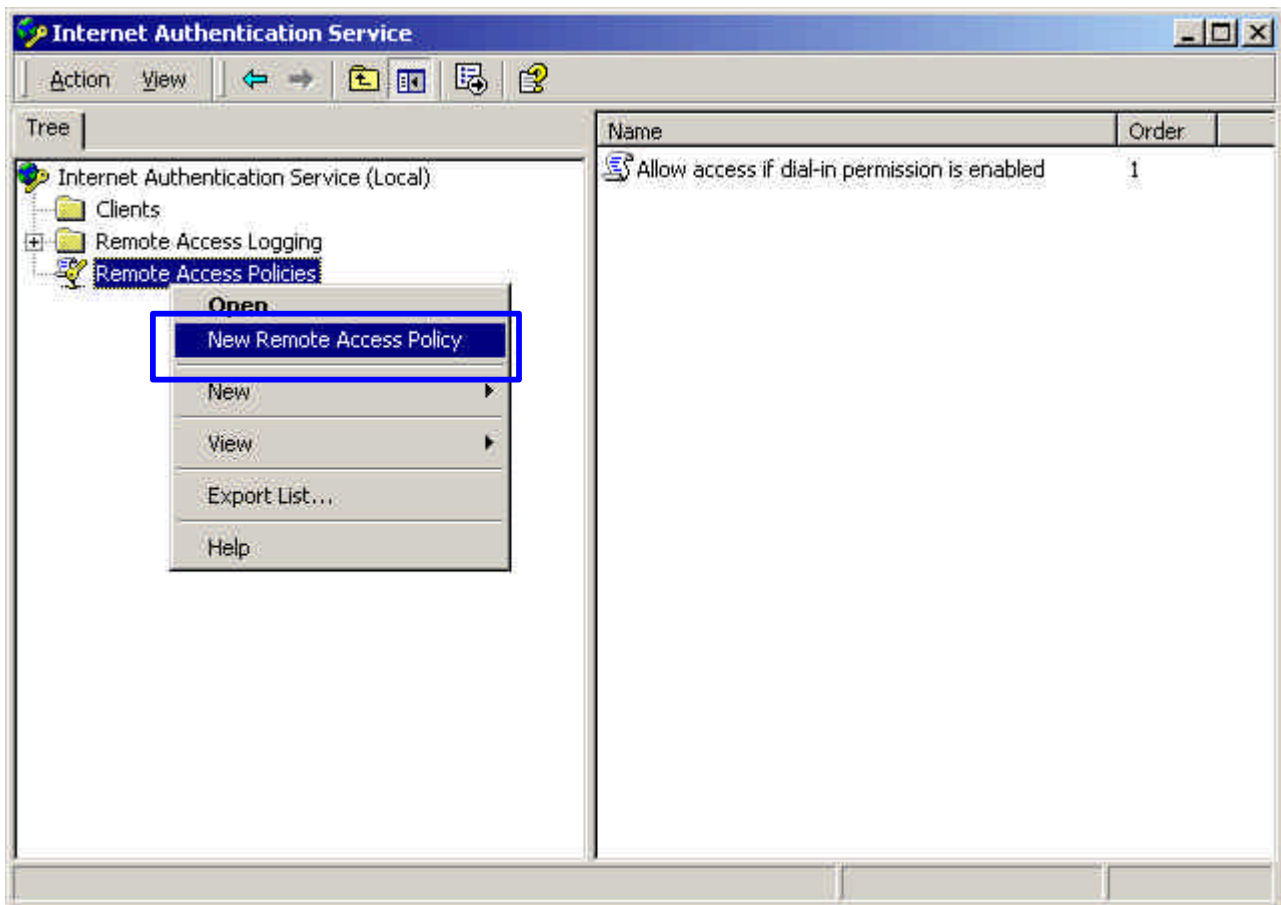
☐ Client must always send the signature attribute in the request

Shared secret: xxxxx

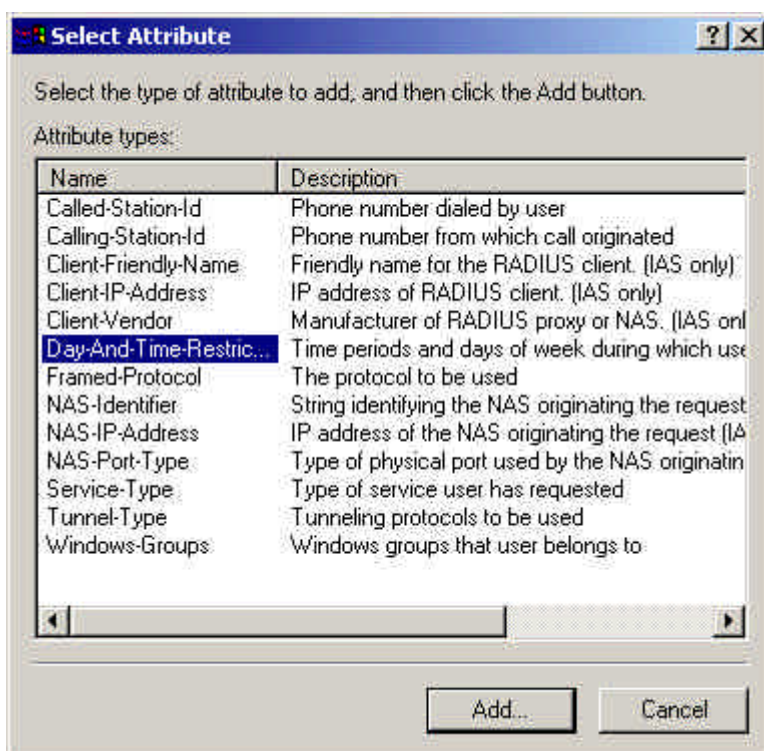
Confirm shared secret: xxxxx

< Back Finish Cancel

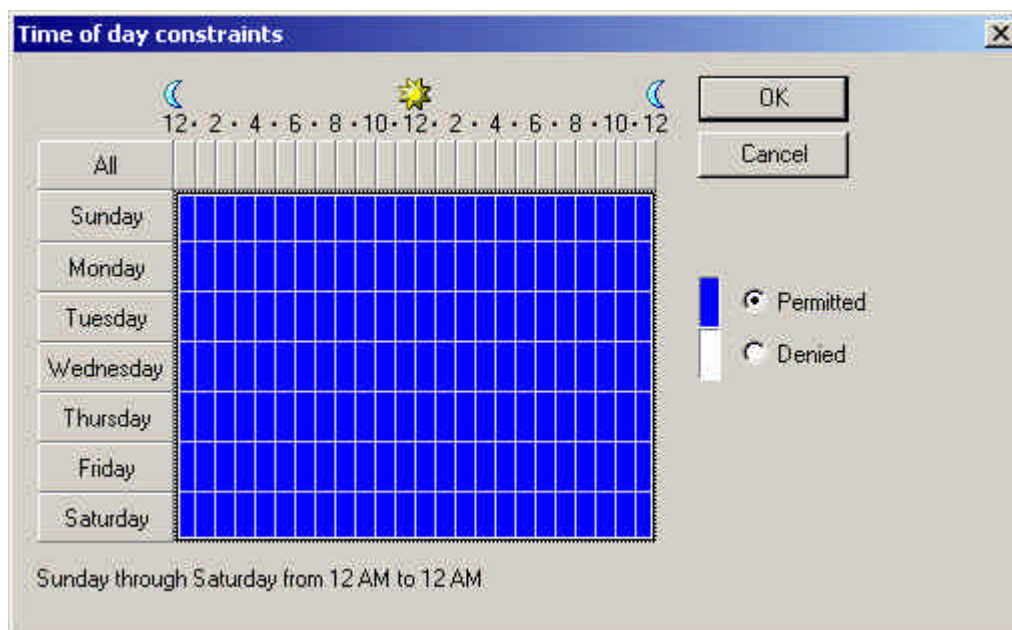
28. In the Internet Authentication Service, right-click **“Remote Access Policies”**
29. Select **“New Remote Access Policy”**.



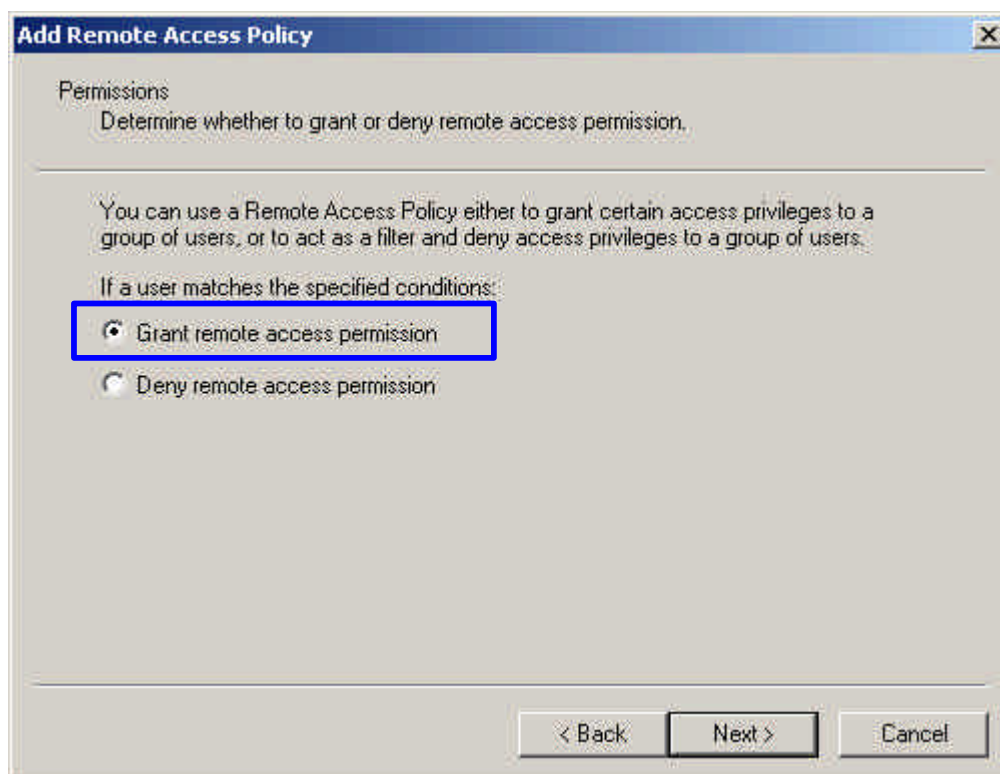
30. Select **“Day-And-Time-Restriction”**, and click **“Add”** to continue.



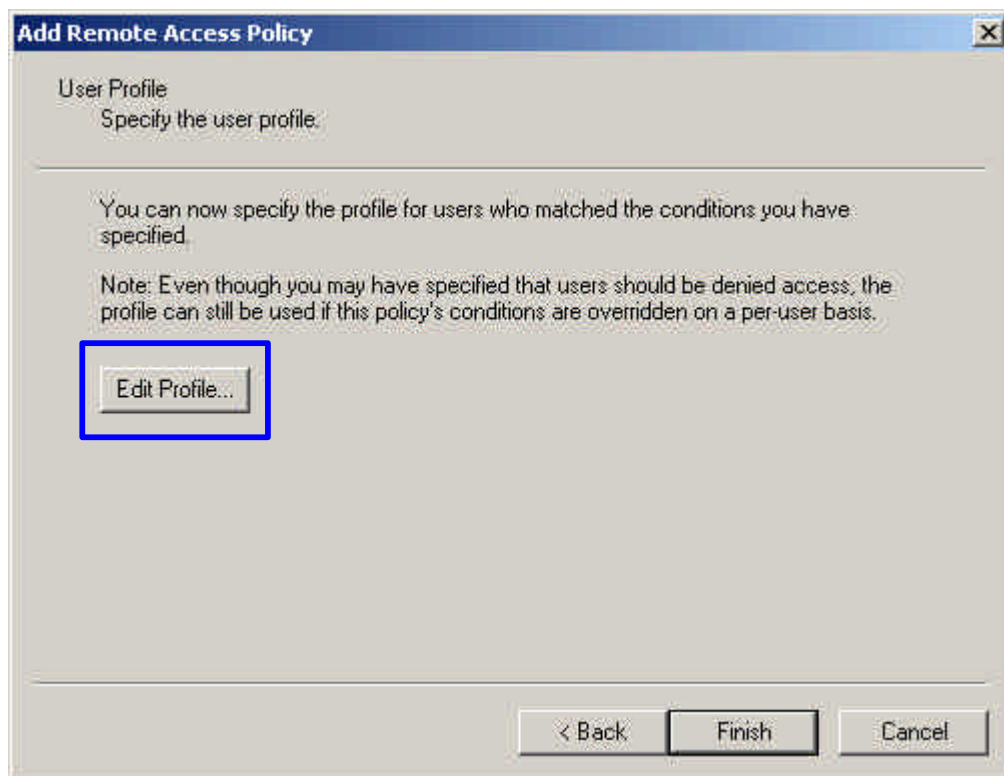
31. Unless you want to specify the active duration for 802.1x authentication, click “OK” to accept to have 802.1x authentication enabled at all times.



32. Select “Grant remote access permission”, and click “Next” to continue.

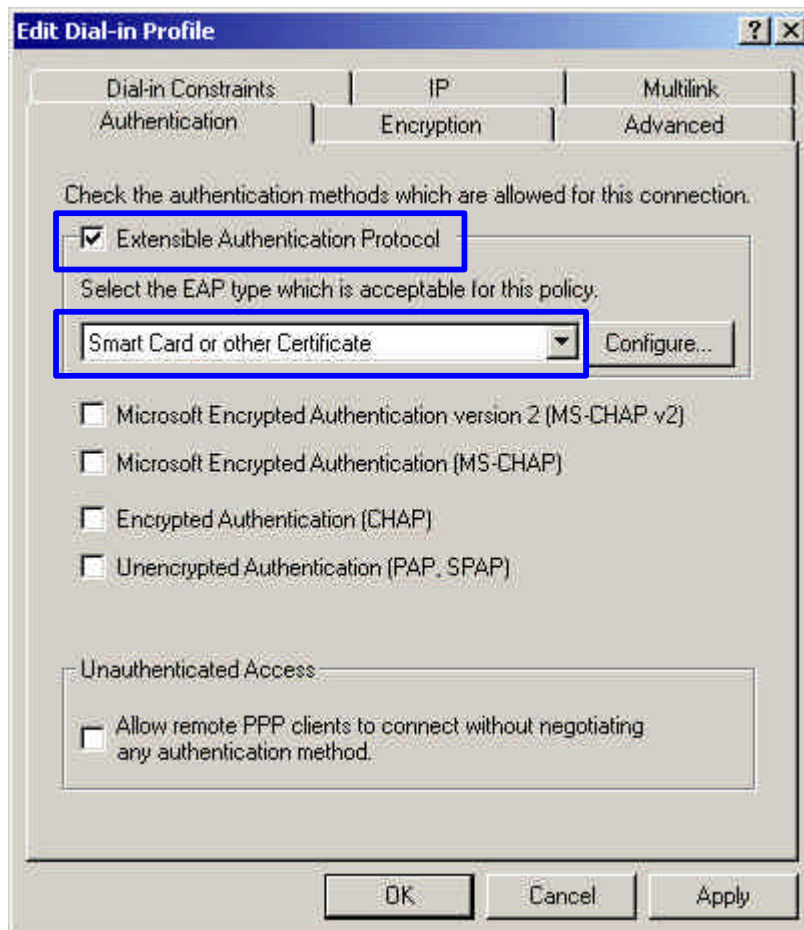


33. Click “Edit Profile” to open up

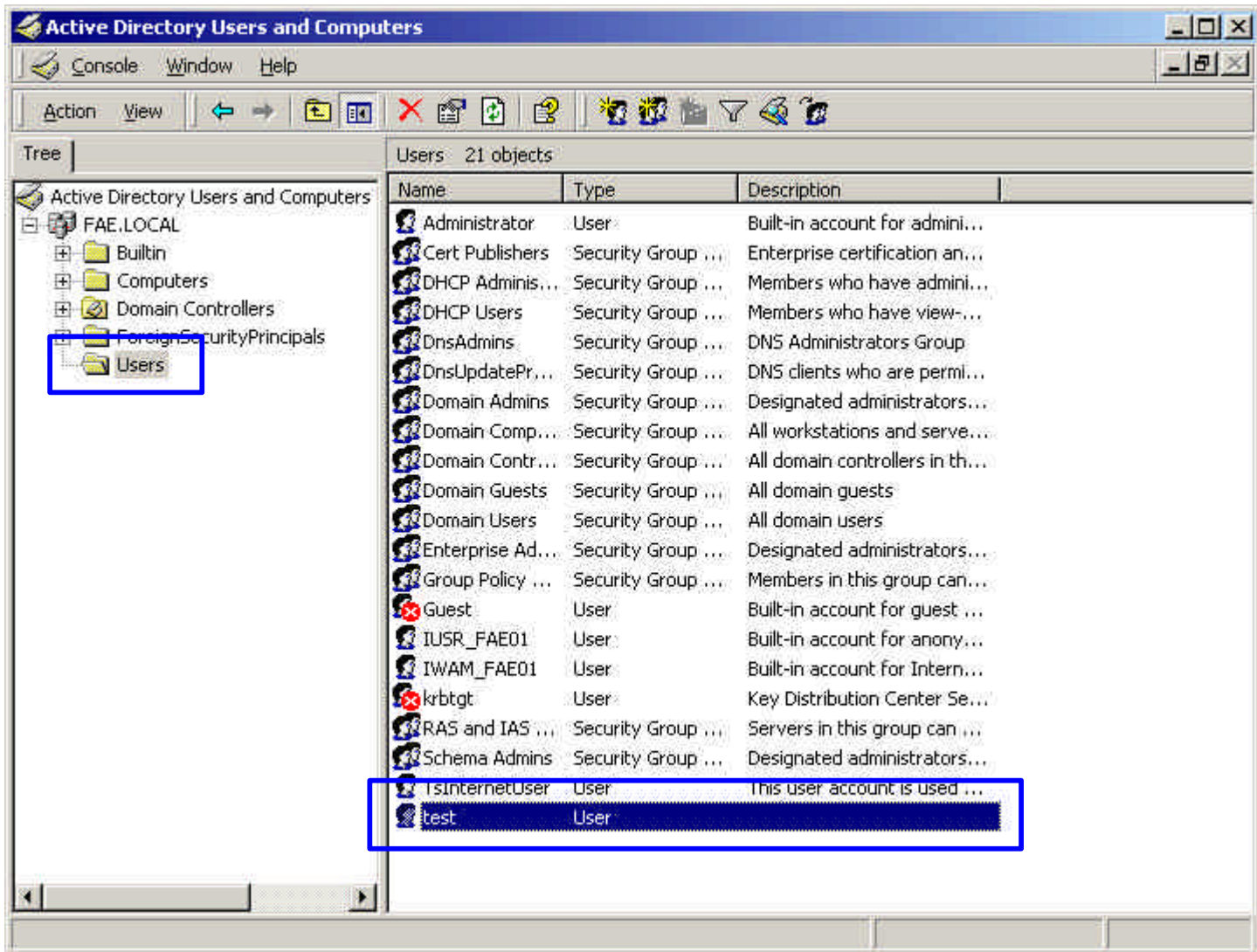


For TLS Authentication Setup (Steps 34 ~ 38)

34. Select “**Authentication**” Tab
35. Enable “**Extensible Authentication Protocol**”, and select “**Smart Card or other Certificate**” for TLS authentication



36. Go to Start > Program > Administrative Tools > **Active Directory Users and Computers**
37. Select “**Users**”, and double-click on the user that can be newly created or currently existing, who will be configured to have the right to obtain digital certificate remotely.



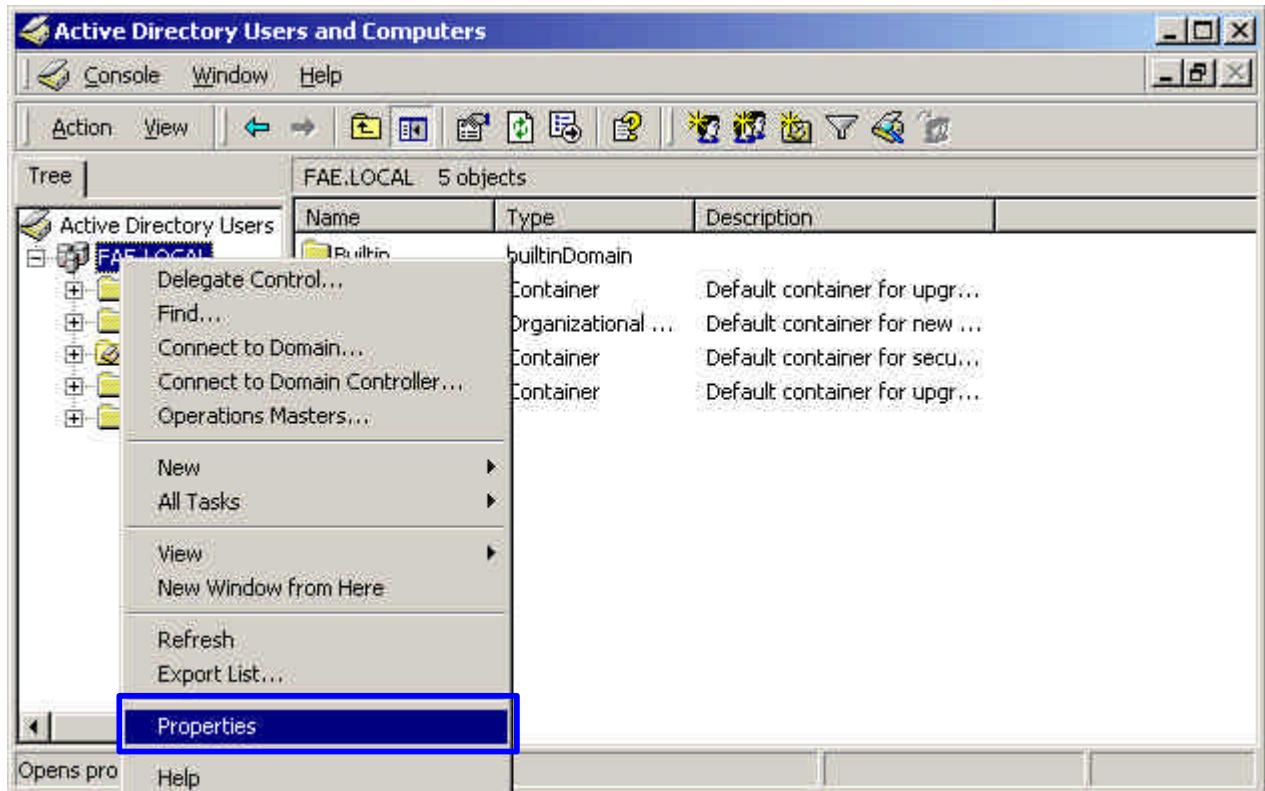
Please note that in this case, we have a user called, **test**, whose account/password are used to obtain the digital certificate from server.

38. Go to the “**Dial-in**” tab, and check “**Allow access**” option for Remote Access Permission and “**No Callback**” for Callback Options.

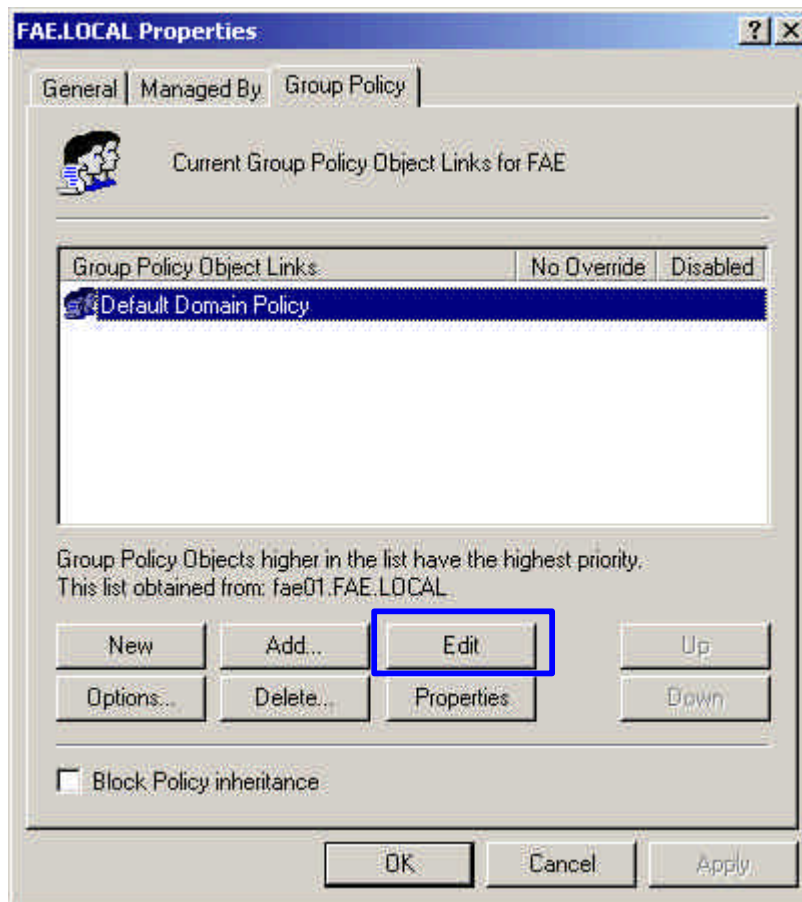
The screenshot shows the 'test Properties' dialog box with the 'Dial-in' tab selected. The 'Dial-in' tab is highlighted with a blue box. The 'Remote Access Permission (Dial-in or VPN)' section has three radio buttons: 'Allow access' (selected, indicated by a blue arrow), 'Deny access', and 'Control access through Remote Access Policy'. The 'Callback Options' section has three radio buttons: 'No Callback' (selected, indicated by a blue arrow), 'Set by Caller (Routing and Remote Access Service only)', and 'Always Callback to:'. There are also checkboxes for 'Verify Caller ID', 'Assign a Static IP Address', and 'Apply Static Routes'. At the bottom, there are 'OK', 'Cancel', and 'Apply' buttons.

For MD5 Authentication (Steps 39 ~ 54)

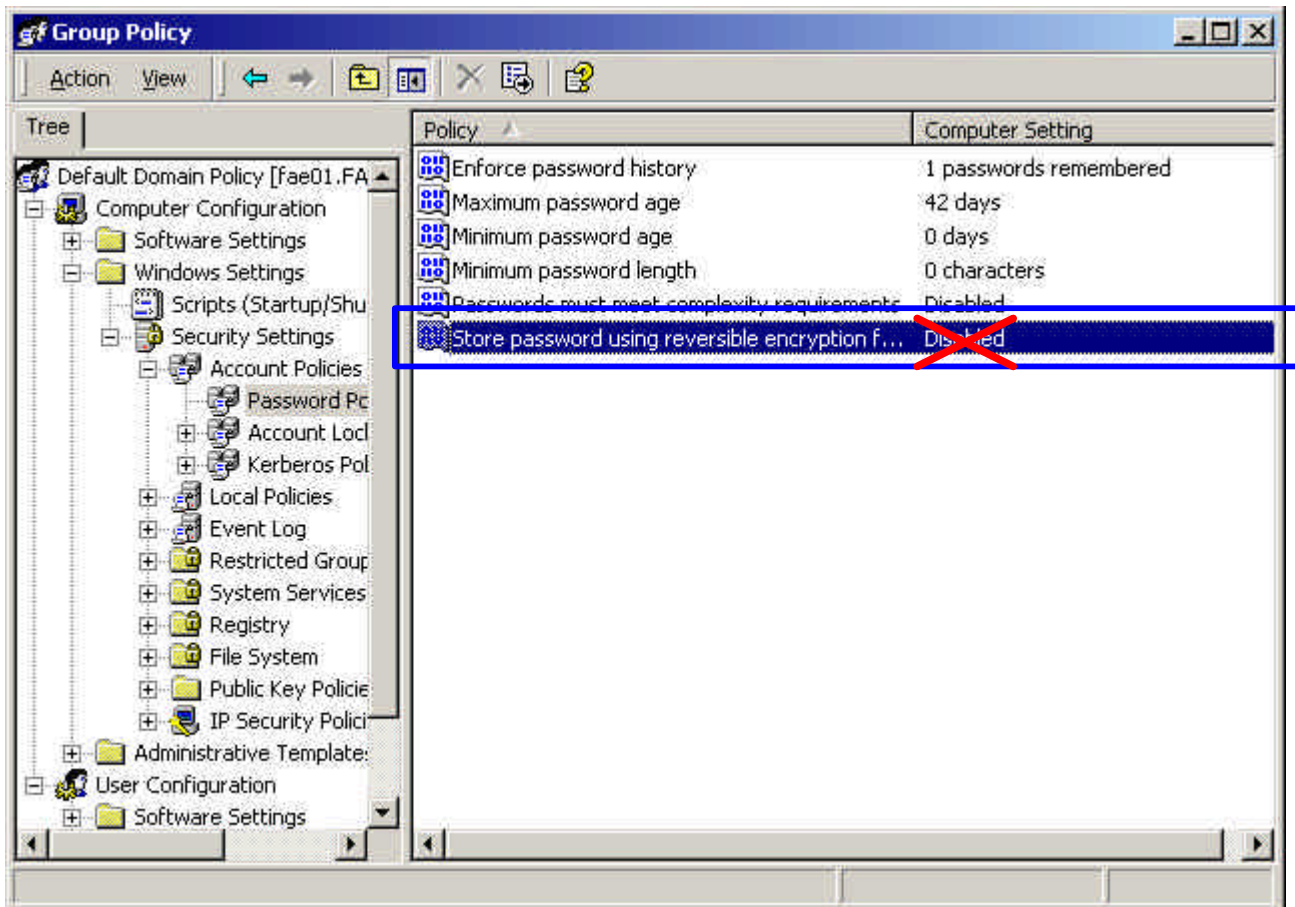
39. Go to Start > Program > Administrative Tools > **Active Directory Users and Computers**.
40. Right click on the domain, and select **“Properties”**



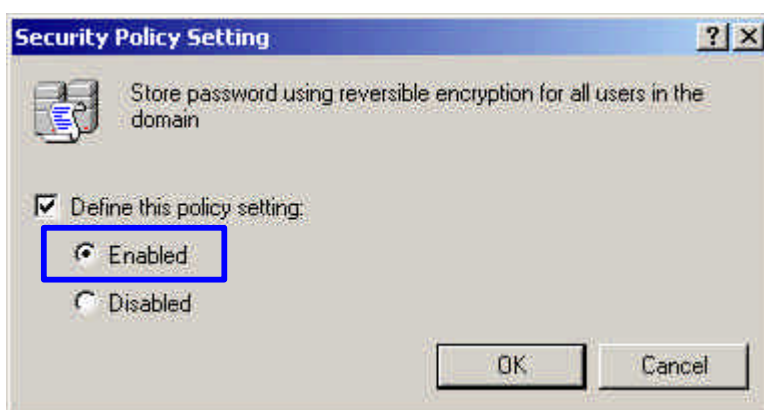
41. Select “**Group Policy**” tab, and click “**Edit**” to edit the Group Policy.



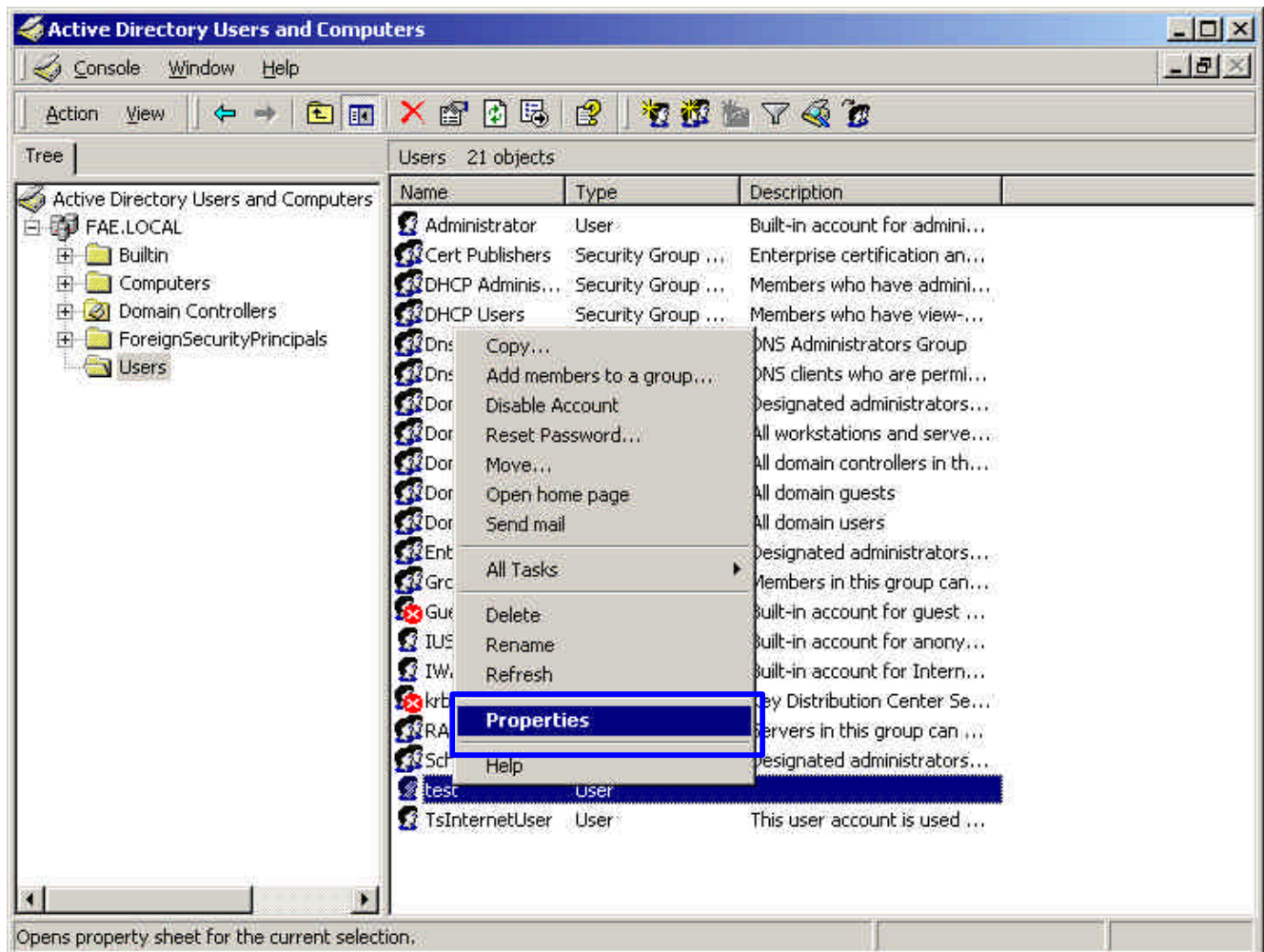
42. Go to “Computer Configuration” > “Windows Settings” > “Security Settings” > “Account Policies” > “**Password Policies**”



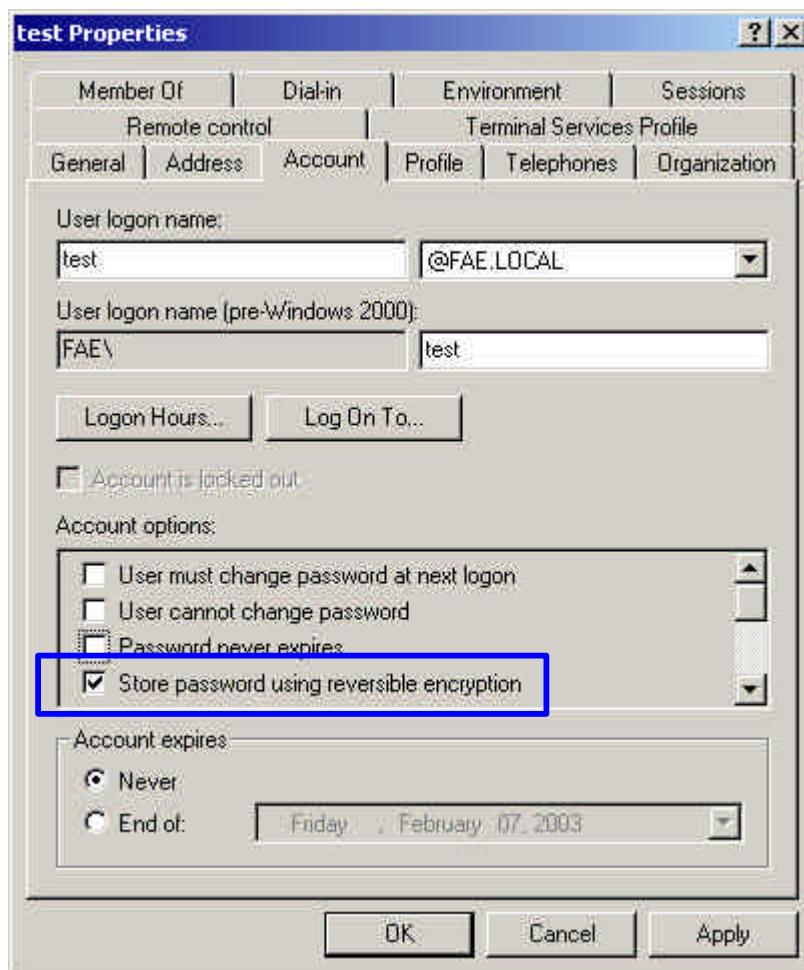
43. Click “**Define this policy setting**”, select “**Enabled**”, and click “**OK**” to continue.



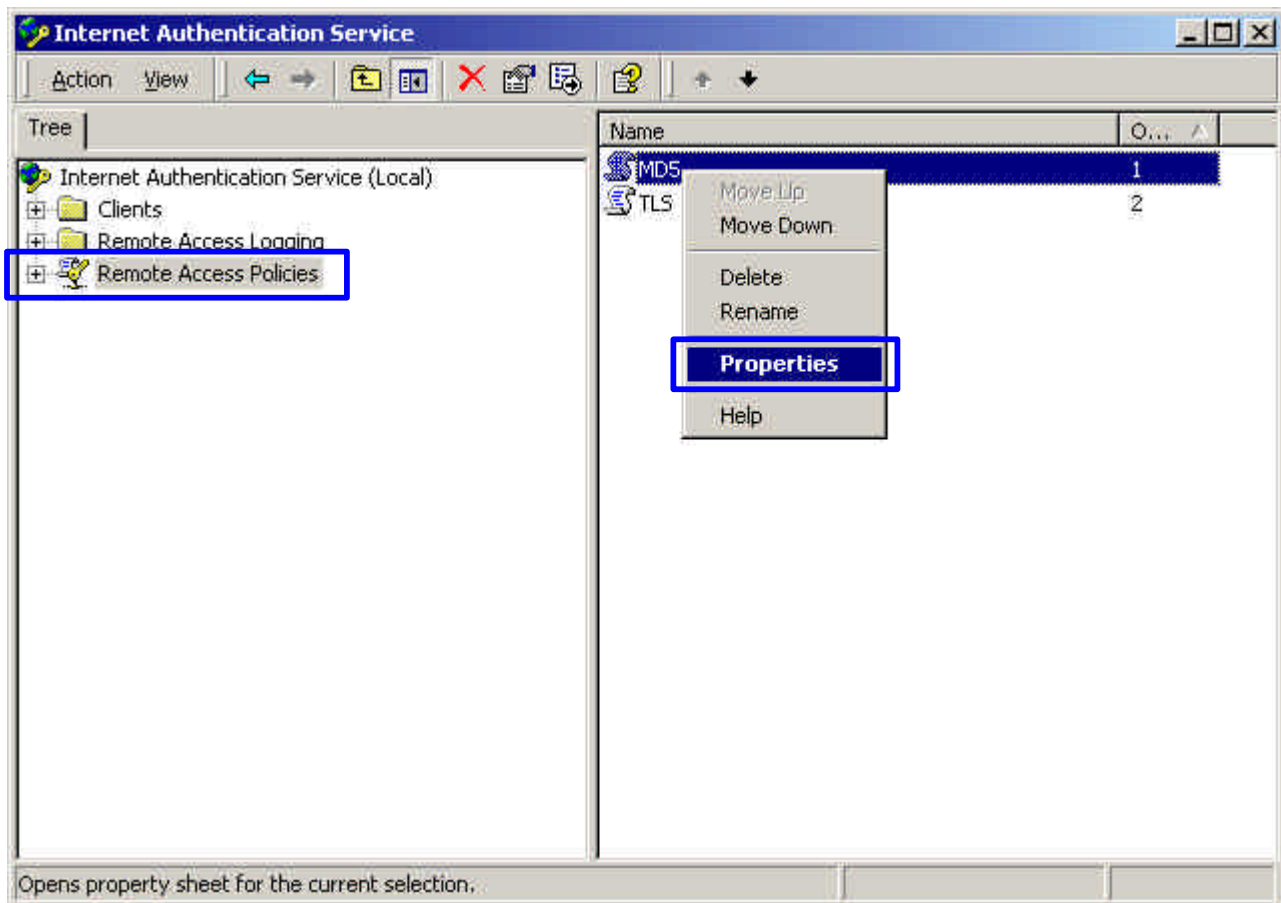
44. Go to Start > Program > Administrative Tools > **Active Directory Users and Computers**.
45. Go to **Users**. Right-click on the user that you are granting access, and select **“Properties”**



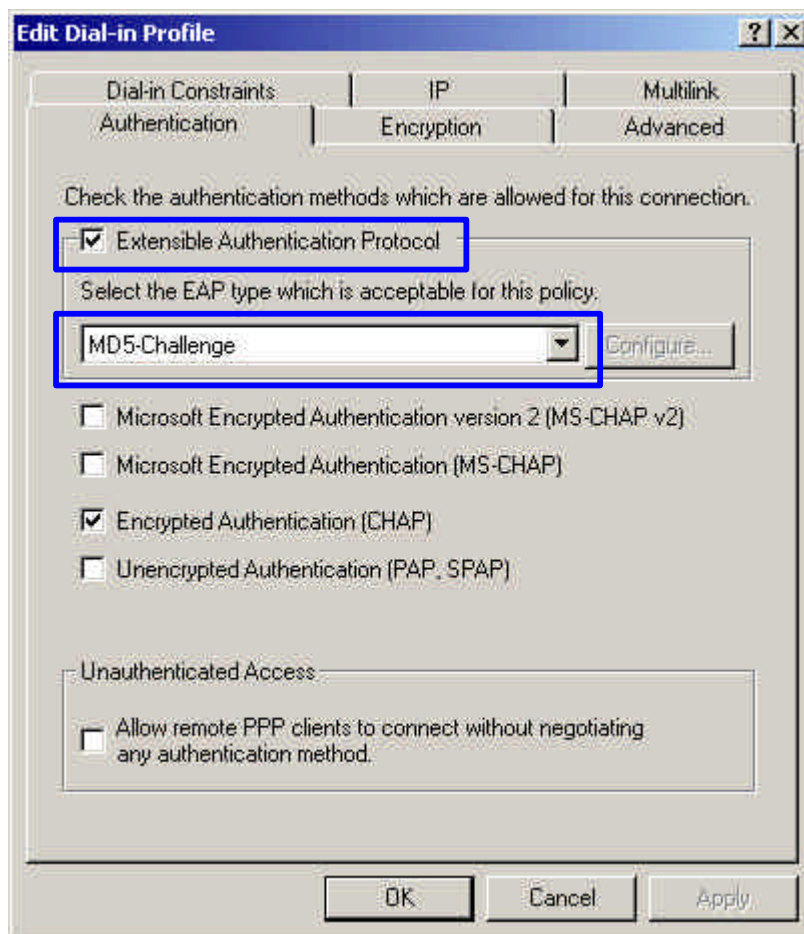
46. Go to “**Account**” tab, and enable “**Store password using reversible encryption**”
47. Click “**OK**” to continue.



48. Go to Start > Program > Administrative Tools > **Internet Authentication Service**.
49. Go to **Remote Access Policies**
50. Make sure that **MD5** is moved up to Order 1
51. Right-click “**MD5**”, and select “**Properties**”



52. Go to “**Authentication**” tab
53. Enable “**Extensible Authentication Protocol**”
54. Select “**MD5-Challenge**” for EAP type.



APPENDIX D: GLOSSARY

Access Point ? An internetworking device that seamlessly connects wired and wireless networks.

Ad-Hoc ? An independent wireless LAN network formed by a group of computers, each with an network adapter.

AP Client – One of the additional AP operating modes offered by 11Mbps Access Point, which allows the Access Point to act as an Ethernet-to-Wireless Bridge, thus a LAN or a single computer station can join a wireless ESS network through it.

ASCII – American Standard Code for Information Interchange, ASCII, is one of the two formats that you can use for entering the values for WEP key. It represents English letters as numbers from 0 to 127.

Authentication Type ? Indication of an authentication algorithm which can be supported by the Access Point:

1. Open System : Open System authentication is the simplest of the available authentication algorithms. Essentially it is a null authentication algorithm. Any station that requests authentication with this algorithm may become authenticated if 802.11 Authentication Type at the recipient station is set to Open System authentication.
2. Shared Key : Shared Key authentication supports authentication of stations as either a member of those who knows a shared secret key or a member of those who does not.

Backbone ? The core infrastructure of a network, which transports information from one central location to another where the information is unloaded into a local system.

Bandwidth ? The transmission capacity of a device, which is calculated by how much data the device can transmit in a fixed amount of time expressed in bits per second (bps).

Basic Rate ? the fixed transmitted and receiving data rate allowed by the AP with the value 1,2,5.5, 11 and 11 Mbps for selection.

Beacon ? A beacon is a packet broadcast by the Access Point to keep the network synchronized. Included in a beacon are information such as wireless LAN service area, the AP address, the Broadcast destination addresses, time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM).

Bit ? A binary digit, which is either -0 or -1 for value, is the smallest unit for data.

Bridge ? An internetworking function that incorporates the lowest 2 layers of the OSI network protocol model.

Browser ? An application program that enables one to read the content and interact in the World Wide Web or Intranet.

BSS ? BSS stands for “Basic Service Set”. It is an Access Point and all the LAN PCs that associated with it.

Channel ? The bandwidth which wireless Radio operates is divided into several segments, which we call them “Channels”. AP and the client stations that it associated work in one of the channels.

CSMA/CA ? In local area networking, this is the CSMA technique that combines slotted time-division multiplexing with carrier sense multiple access/collision detection (CSMA/CD) to avoid having collisions occur a second time. This works best if the time allocated is short compared to packet length and if the number of situations is small.

CSMA/CD ? Carrier Sense Multiple Access/Collision Detection, which is a LAN access method used in Ethernet. When a device wants to gain access to the network, it checks to see if the network is quiet (senses the carrier). If it is not, it waits a random amount of time before retrying. If the network is quiet and two devices access the line at exactly the same time, their signals collide. When the collision is detected, they both back off and wait a random amount of time before retrying.

DHCP ? Dynamic Host Configuration Protocol, which is a protocol that lets network administrators manage and allocate Internet Protocol (IP) addresses in a network. Every computer has to have an IP address in order to communicate with each other in a TCP/IP based infrastructure network. Without DHCP, each computer must be entered in manually the IP address. DHCP enables the network administrators to assign the IP from a central location and each computer receives an IP address upon plugged with the Ethernet cable everywhere on the network.

DSSS ? Direct Sequence Spread Spectrum. DSSS generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for

retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

Dynamic IP Address ? An IP address that is assigned automatically to a client station in a TCP/IP network by a DHCP server.

Encryption ? A security method that uses a specific algorithm to alter the data transmitted, thus prevent others from knowing the information transmitted.

ESS ? ESS stands for “Extended Service Set”. More than one BSS is configured to become Extended Service Set. LAN mobile users can roam between different BSSs in an ESS.

ESSID ? The unique identifier that identifies the ESS. In infrastructure association, the stations use the same ESSID as AP’s to get connected.

Ethernet ? A popular local area data communications network, originally developed by Xerox Corp., that accepts transmission from computers and terminals. Ethernet operates on a 10/100 Mbps base transmission rate, using a shielded coaxial cable or over shielded twisted pair telephone wire.

Fragmentation ? When transmitting a packet over a network medium, sometimes the packet is broken into several segments, if the size of packet exceeds that allowed by the network medium.

Fragmentation Threshold – The Fragmentation Threshold defines the number of bytes used for the fragmentation boundary for directed messages. The purpose of "Fragmentation Threshold" is to increase the transfer reliability thru cutting a MAC Service Data Unit (MSDU) into several MAC Protocol Data Units (MPDU) in smaller size. The RF transmission can not allow to transmit too big frame size due to the heavy interference caused by the big size of transmission frame. But if the frame size is too small, it will create the overhead during the transmission.

Gateway ? a device that interconnects networks with different, incompatible communication protocols.

HEX – Hexadecimal, HEX, consists of numbers from 0 – 9 and letters from A – F.

IEEE ? The Institute of Electrical and Electronics Engineers, which is the largest technical professional society that promotes the development and application of electrotechnology and allied sciences for the benefit of humanity, the advancement of the profession. The IEEE fosters the development of standards that often become national and international standards.

Infrastructure ? An infrastructure network is a wireless network or other small network in which the wireless network devices are made a part of the network through the Access Point which connects them to the rest of the network.

ISM Band ? The FCC and their counterparts outside of the U.S. have set aside

bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4GHz, in particular, is being made available worldwide.

MAC Address ? Media Access Control Address is a unique hex number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level.

Multicasting ? Sending data to a group of nodes instead of a single destination.

Multiple Bridge – One of the additional AP operating modes offered by 11Mbps Access Point, which allows a group of APs that consists of two or more APs to connect two or more Ethernet networks or Ethernet enabled clients together. The way that multiple bridge setup is based on the topology of Ad-Hoc mode.

Node ? A network junction or connection point, typically a computer or workstation.

Packet ? A unit of data routed between an origin and a destination in a network.

PLCP ? Physical layer convergence protocol

PPDU ? PLCP protocol data unit

Preamble Type ? During transmission, the PSDU shall be appended to a PLCP preamble and header to create the PPDU. Two different preambles and headers are defined as the mandatory supported long preamble and header which interoperates with the current 1 and 2 Mbit/s DSSS specification as described in IEEE Std 802.11-1999, and an optional short preamble and header. At the receiver, the PLCP preamble and header are processed to aid in demodulation and delivery of the PSDU. The optional short preamble and header is intended for application where maximum throughput is desired and interoperability with legacy and non-short-preamble capable equipment is not consideration. That is, it is expected to be used only in networks of like equipment that can all handle the optional mode. (IEEE 802.11b standard)

PSDU ? PLCP service data unit

Roaming ? A LAN mobile user moves around an ESS and enjoys a continuous connection to an Infrastructure network.

RTS ? Request To Send. An RS-232 signal sent from the transmitting station to the receiving station requesting permission to transmit.

RTS Threshold ? Transmitters contending for the medium may not be aware of each other. RTS/CTS mechanism can solve this “Hidden Node Problem”. If the packet size is smaller than the preset RTS Threshold size, the RTS/CTS mechanism will NOT be enabled.

SSID ? Service Set Identifier, which is a unique name shared among all clients and nodes in a wireless network. The SSID must be identical for each clients and nodes in the wireless network.

Subnet Mask ? The method used for splitting IP networks into a series of sub-groups, or subnets. The mask is a binary pattern that is matched up with the IP address to turn part of the host ID address field into a field for subnets.

TCP/IP ? Transmission Control Protocol/ Internet Protocol. The basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network, i.e. intranet or internet. When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

Throughput ? The amount of data transferred successfully from one point to another in a given period of time.

WEP ? Wired Equivalent Privacy (WEP) is an encryption scheme used to protect wireless data communication. To enable the icon will prevent other stations without the same WEP key from linking with the AP.

Wireless Bridge – One of the additional AP operating modes offered by 11mpbs Access Point, which allows a pair of APs to act as the bridge that connects two Ethernet networks or Ethernet enabled clients together.

APPENDIX E: TECHNICAL SPECIFICATION

Standard	802.11b compliant (wireless)	
Data Rate	1 / 2 / 5.5 / 11 Mbps	
Emission Type	Direct Sequence Spread Spectrum (DSSS)	
Data Modulation	1 Mbps – BPSK	
	2 Mbps – QPSK	
	5.5 / 11 Mbps – CCK	
RF Frequency	2412 MHz – 2462 MHz (North America)	
	2412 MHz – 2472 MHz (General Europe)	
	2412 MHz – 2484 MHz (Japan)	
Operating Channel	11 Channels (North America)	
	13 Channels (Europe)	
	14 Channels (Japan)	
RF Output Power	16 dBm (typical)	
Sensitivity	1, 2Mbps BPSK, QPSK	-92 dBm
	5.5Mbps CCK	-88 dBm
	11Mbps CCK	-84 dBm
	(typically @PER < 8% packet size 1024 and @25°C ± 5°C)	
Security	Wired Equivalent Privacy (WEP) 64 / 128bit	
Antenna Type	Diversity Patch with 2.0 dBi max. Antenna Gain.	
Interface	PCIBus, PCI Standard v7.2	
Dimension	114 x 54 x 5 mm	
Memory	8Kbytes EEPROM	
Power Voltage	3.3V ± 5%	
Power Consumption	Operation max. 650 mA by TX	
	350 mA by RX	