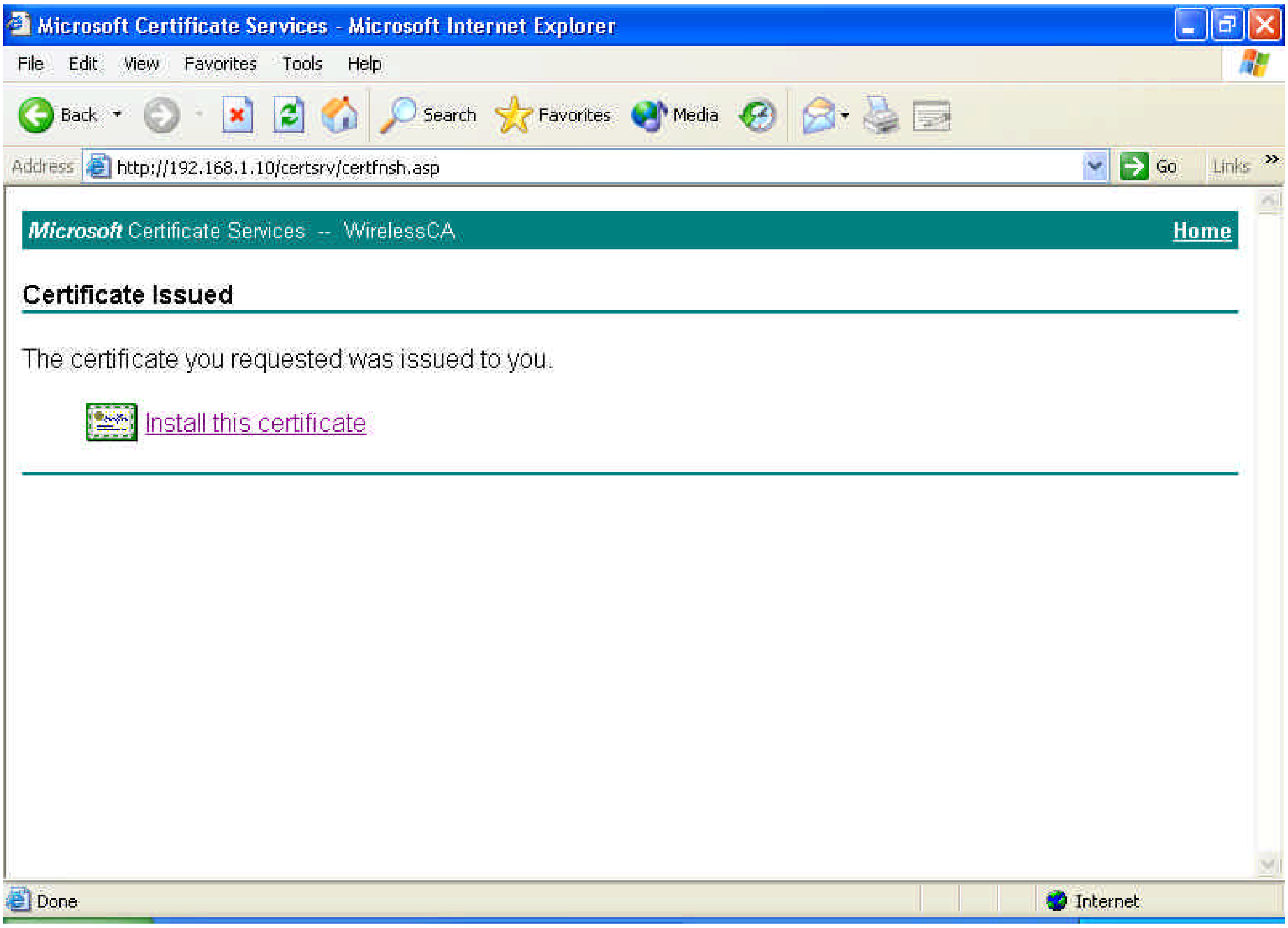
20. The certificate is issued by the server, click “Install this certificate” to download and store the certificate to your local computer.



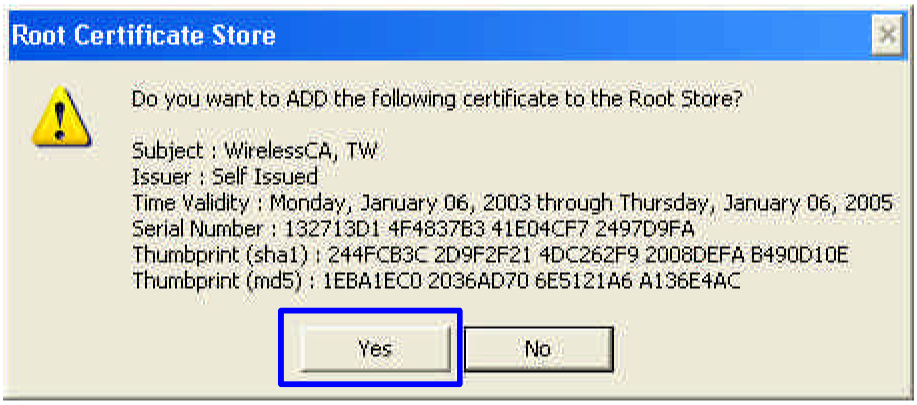
Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.10/certsrv/certfnsh.asp
Go Links
Microsoft Certificate Services -- WirelessCA
Home
Done
Internet

Certificate Issued

The certificate you requested was issued to you.

Install this certificate

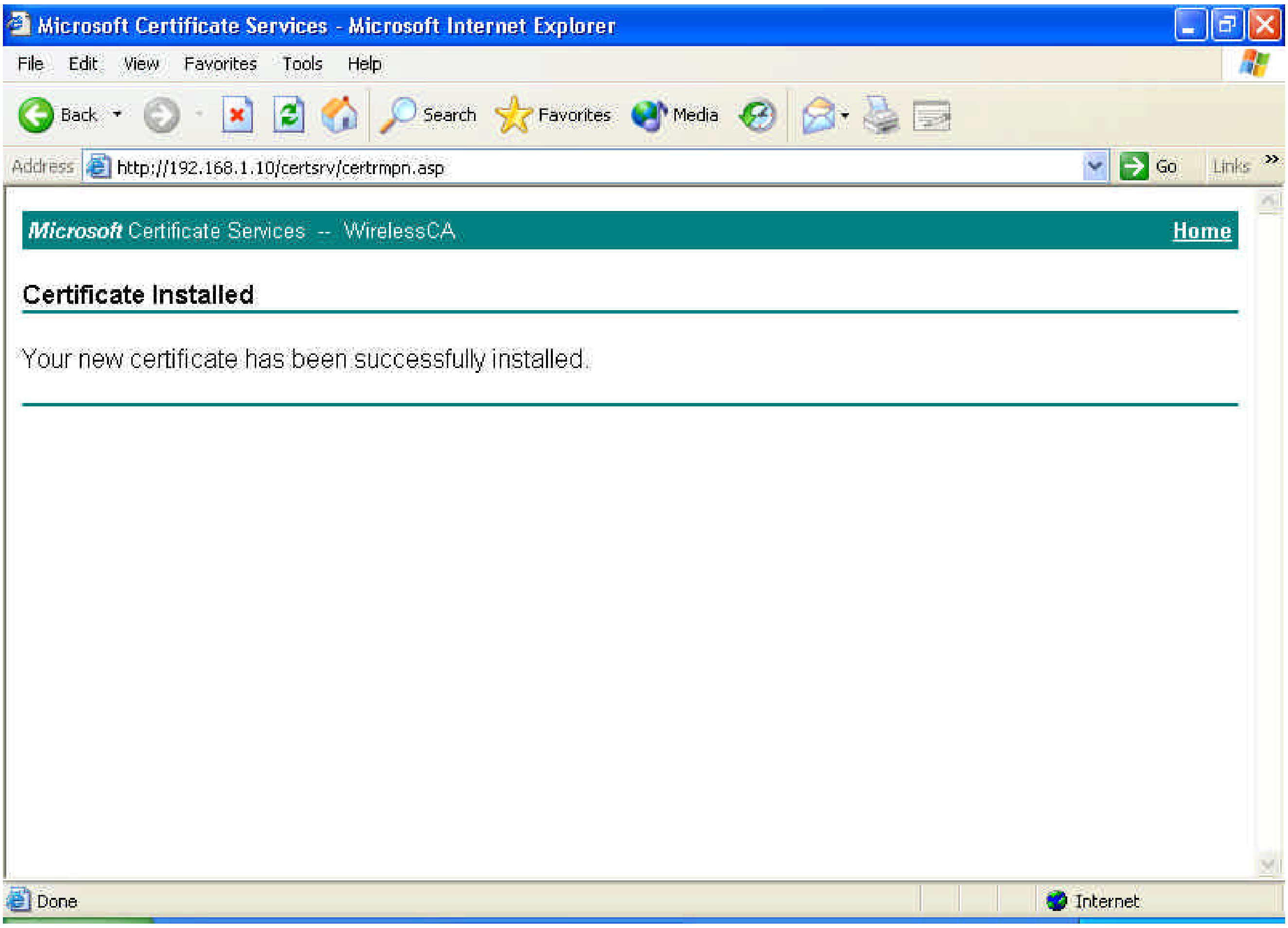
21. Click “**Yes**” to store the certificate to your local computer.



Do you want to ADD the following certificate to the Root Store?

Subject : WirelessCA, TW
Issuer : Self Issued
Time Validity : Monday, January 06, 2003 through Thursday, January 06, 2005
Serial Number : 132713D1 4F4837B3 41E04CF7 2497D9FA
Thumbprint (sha1) : 244FCB3C 2D9F2F21 4DC262F9 2008DEFA B490D10E
Thumbprint (md5) : 1EBA1EC0 2036AD70 6E5121A6 A136E4AC

22. Certificate is now installed.



Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.10/certsrv/certrmpn.asp
Go Links
Done
Internet

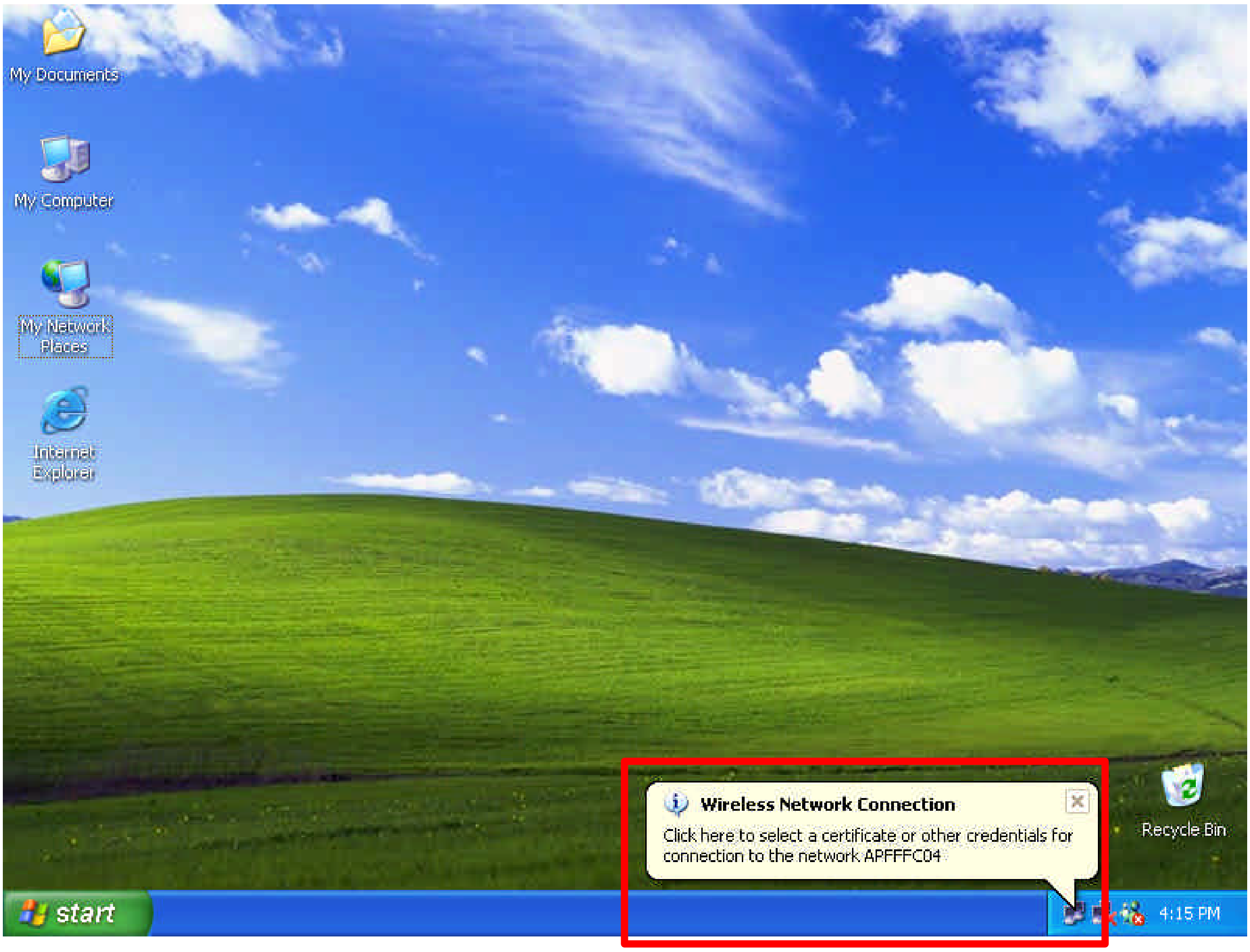
*Microsoft* Certificate Services -- WirelessCA Home

Certificate Installed

Your new certificate has been successfully installed.

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

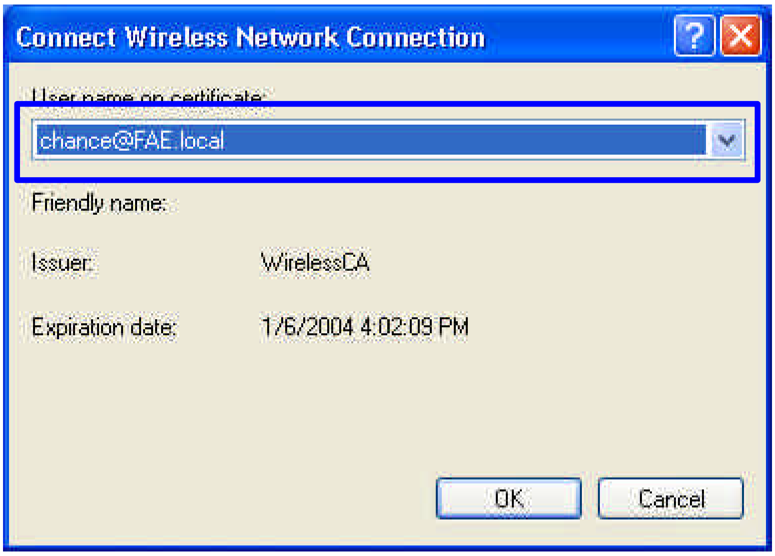
23. Windows XP will prompt you to select a certificate for wireless network connection. Click on the network connection icon in the system tray to continue.



Wireless Network Connection

Click here to select a certificate or other credentials for connection to the network APFFFC04

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



Connect Wireless Network Connection

User name on certificate:

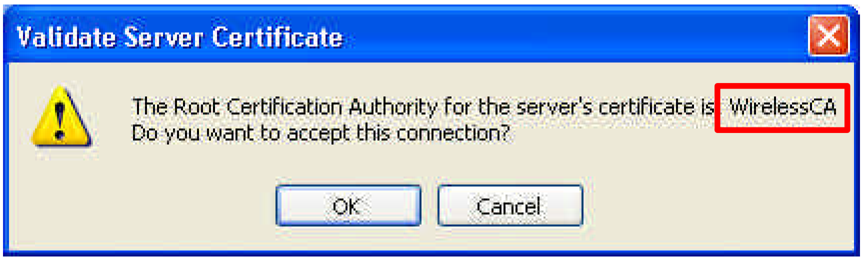
chance@FAE.local

Friendly name:

Issuer: WirelessCA

Expiration date: 1/6/2004 4:02:09 PM

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



Validate Server Certificate

The Root Certification Authority for the server's certificate is WirelessCA
Do you want to accept this connection?

## 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

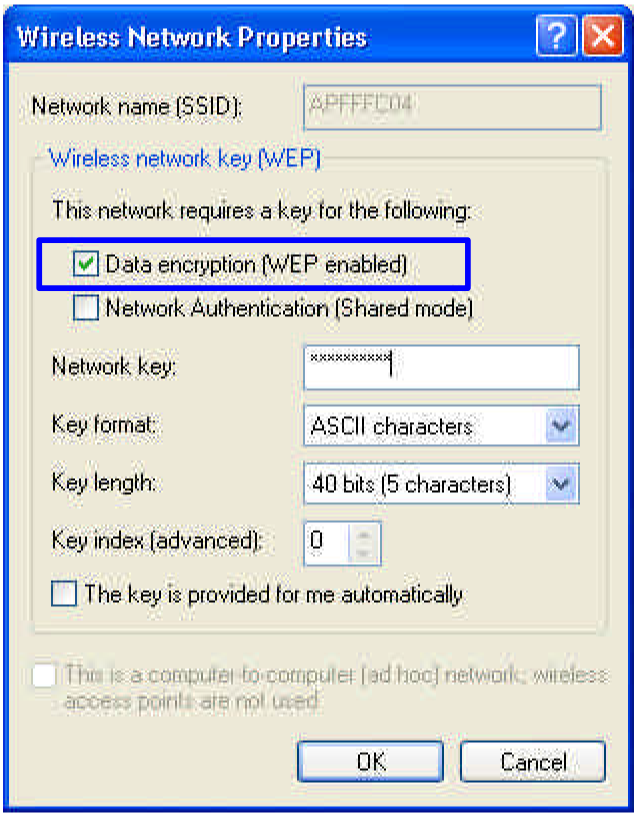
    **HEX** characters: 0~9, a~f

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.


Wireless Network Properties
Wireless network key (WEP)
This network requires a key for the following:
OK
Cancel

Network name (SSID): APFFFC04

☑ Data encryption (WEP enabled)

□ Network Authentication (Shared mode)

Network key: **********

Key format: ASCII characters

Key length: 40 bits (5 characters)

Key index (advanced): 0

□ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

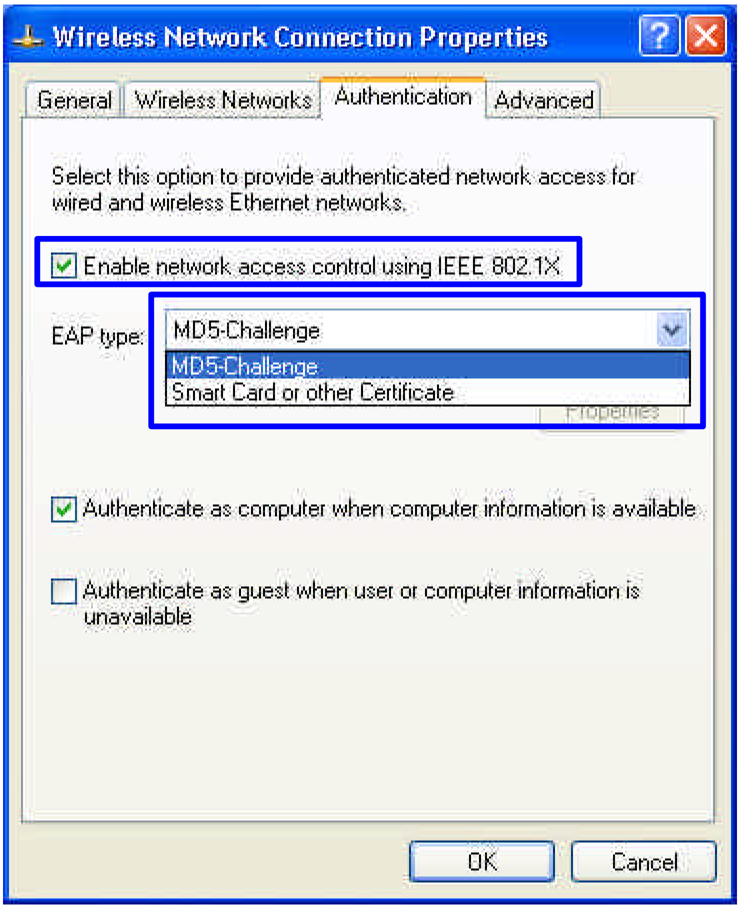
Please note that that value of Network key entered, and key format/length used, must be the same as that used in the Access Point. Although there are 4 set of keys can be set in the Access Point WEP configuration, it’s the ***first set*** of key that must be the same as that we used by the supplicant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



Wireless Network Connection Properties

Select this option to provide authenticated network access for wired and wireless Ethernet networks.

☑ Enable network access control using IEEE 802.1X

EAP type: MD5-Challenge

MD5-Challenge
Smart Card or other Certificate

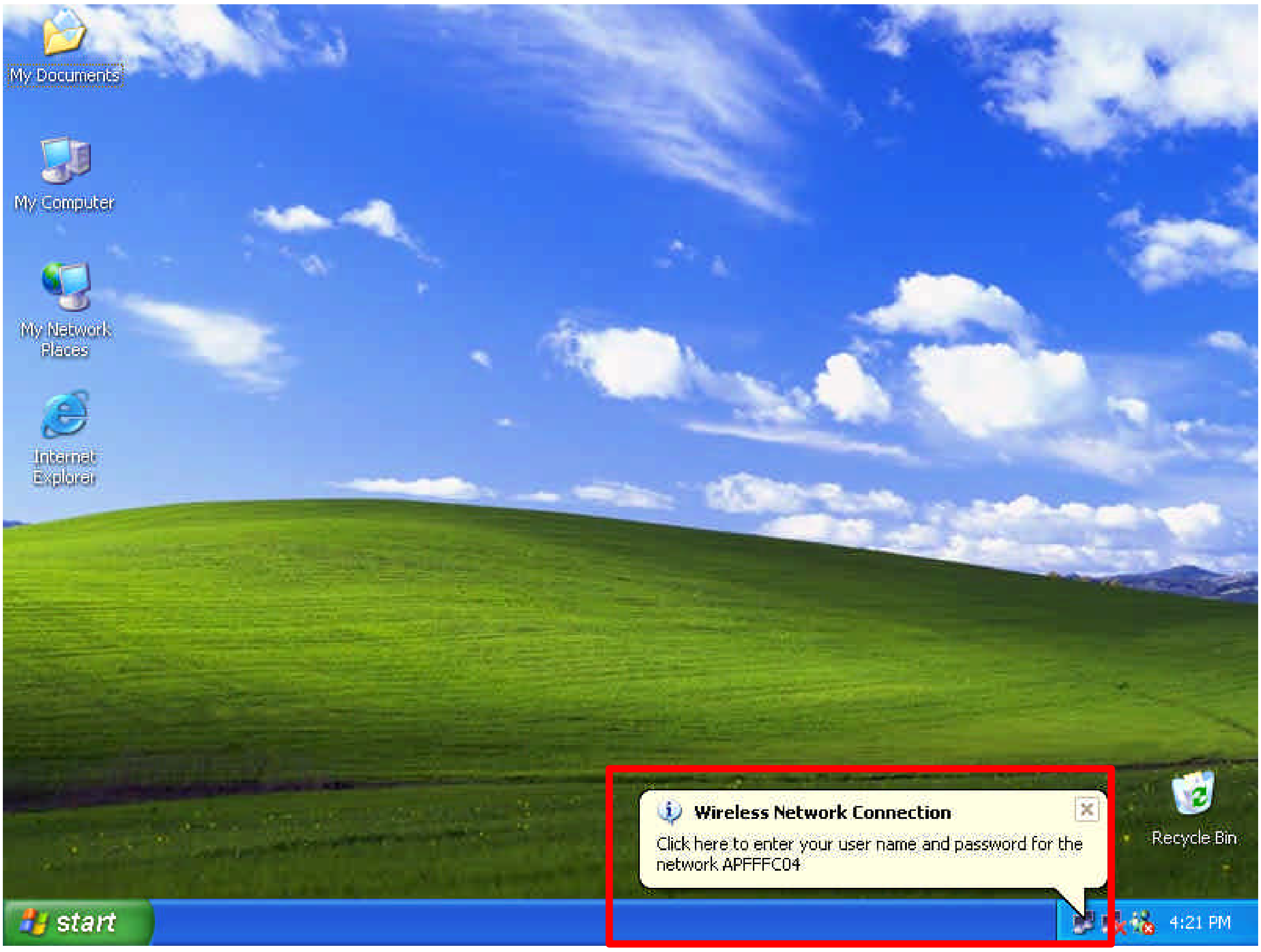
☑ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

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.

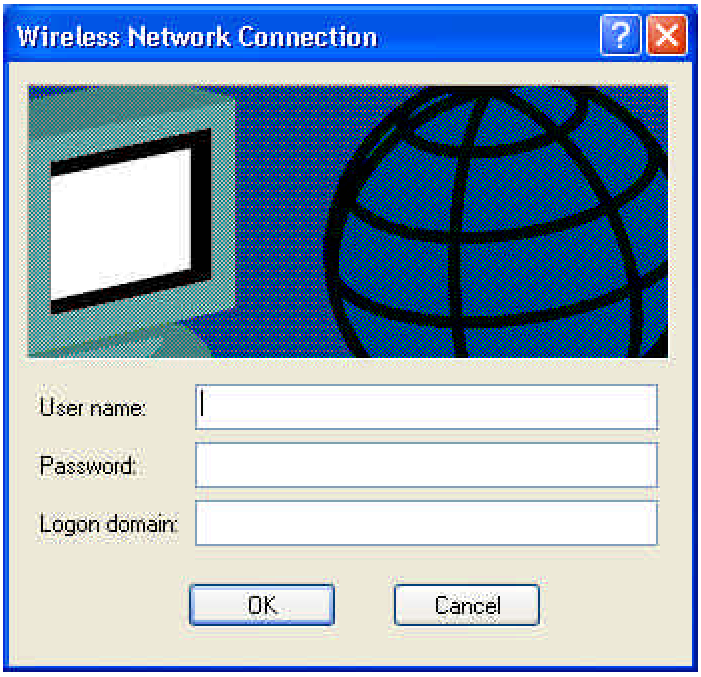


Wireless Network Connection

Click here to enter your user name and password for the network APFFFC04

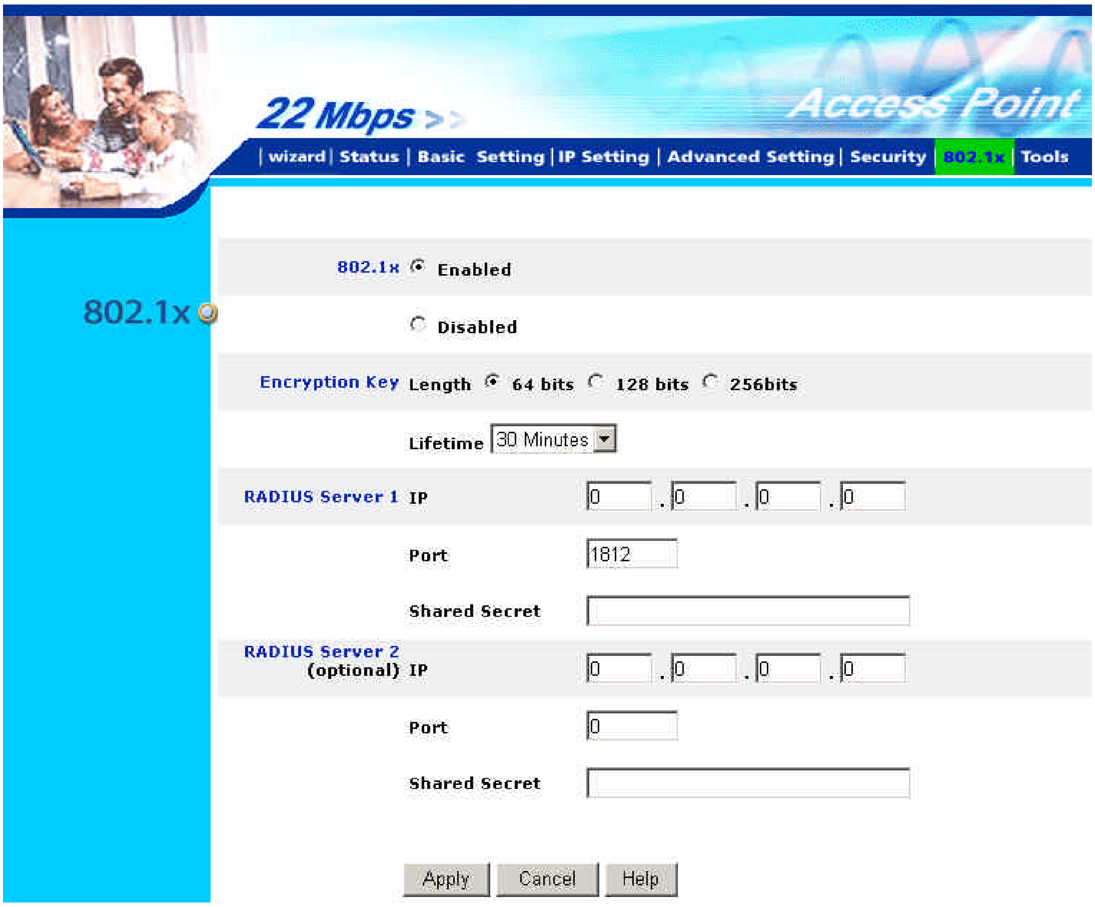
36. Enter the user name, password and the logon domain that your account belongs if you have one or more network domain exist in your network.

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.


22 Mbps >>
Access Point
| wizard | Status | Basic Setting | IP Setting | Advanced Setting | Security | 802.1x | Tools
802.1x

802.1x ● Enabled

○ Disabled

Encryption Key Length ● 64 bits ○ 128 bits ○ 256bits

Lifetime 30 Minutes

RADIUS Server 1 IP 0 . 0 . 0 . 0

Port 1812

Shared Secret

RADIUS Server 2 (optional) IP 0 . 0 . 0 . 0

Port 0

Shared Secret

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

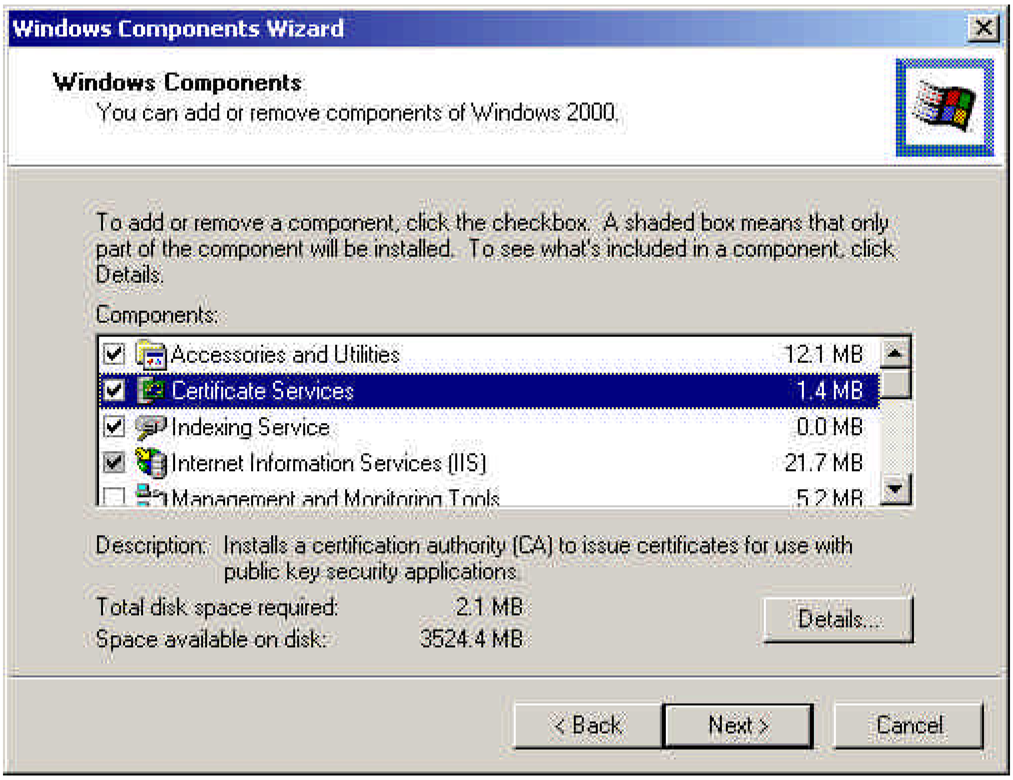
   Enter the **Shared Secret**, which is used by the Radius Server.
5. Enter the **IP address** of, **Port** and **Shared Secret** used by the **Secondary** Radius Server.
6. Click "**Apply**" button for the 802.1x settings to take effect after Access Point reboots itself.

**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.



Windows Components Wizard

Windows Components

You can add or remove components of Windows 2000.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

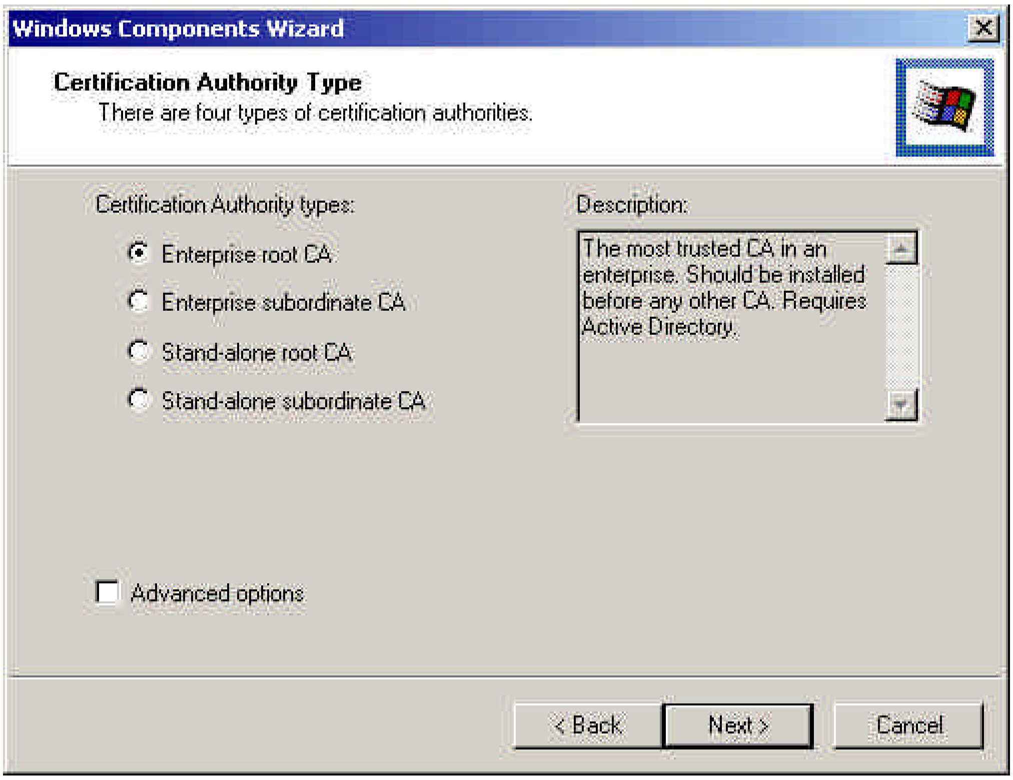
Components:

☑ Accessories and Utilities 12.1 MB
☑ Certificate Services 1.4 MB
☑ Indexing Service 0.0 MB
☑ Internet Information Services (IIS) 21.7 MB
□ Management and Monitoring Tools 5.2 MB

Description: Installs a certification authority (CA) to issue certificates for use with public key security applications.

Total disk space required: 2.1 MB
Space available on disk: 3524.4 MB

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



Windows Components Wizard

**Certification Authority Type**

There are four types of certification authorities.

Certification Authority types:

● Enterprise root CA

○ Enterprise subordinate CA

○ Stand-alone root CA

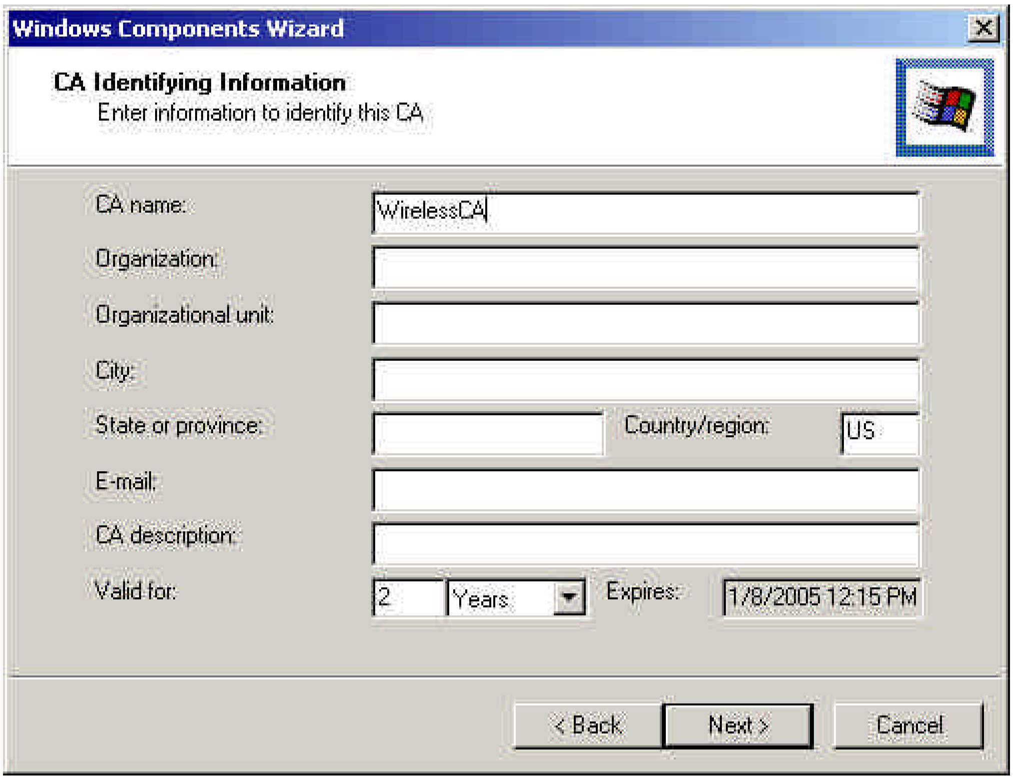
○ Stand-alone subordinate CA

Description:

The most trusted CA in an enterprise. Should be installed before any other CA. Requires Active Directory.

□ Advanced options

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



Windows Components Wizard

**CA Identifying Information**

Enter information to identify this CA

CA name: WirelessCA

Organization:

Organizational unit:

City:

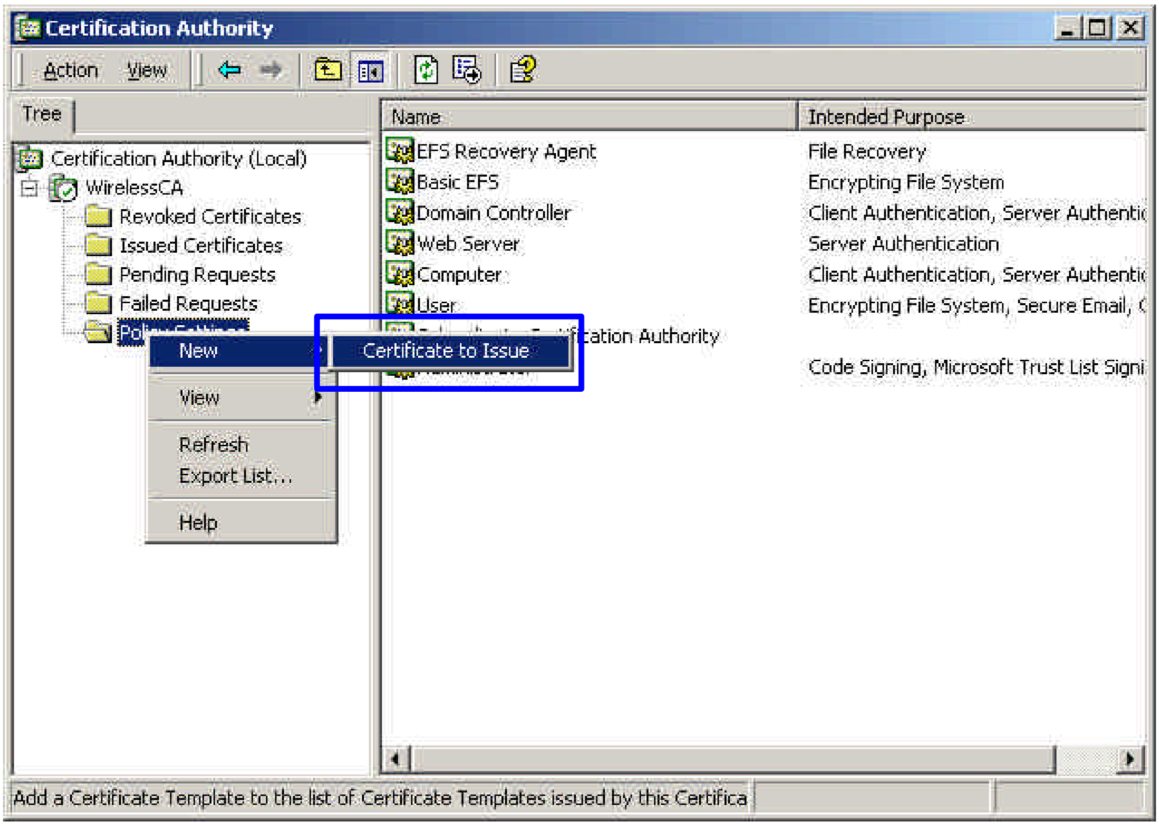
State or province: Country/region: US

E-mail:

CA description:

Valid for: 2 Years Expires: 1/8/2005 12:15 PM

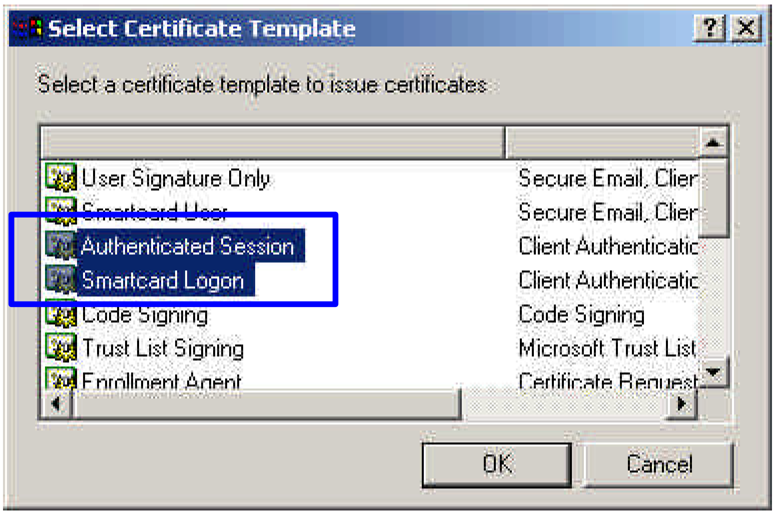
7. Go to Start > Program > Administrative Tools > **Certificate Authority**
8. Right-click on the "**Policy Setting**", select "**new**"
9. Select "**Certificate to Issue**"



| Name | Intended Purpose |
|---|---|
| EFS Recovery Agent | File Recovery |
| Basic EFS | Encrypting File System |
| Domain Controller | Client Authentication, Server Authentic |
| Web Server | Server Authentication |
| Computer | Client Authentication, Server Authentic |
| User | Encrypting File System, Secure Email, C |
| …ation Authority | |
| | Code Signing, Microsoft Trust List Signi |

Add a Certificate Template to the list of Certificate Templates issued by this Certifica

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

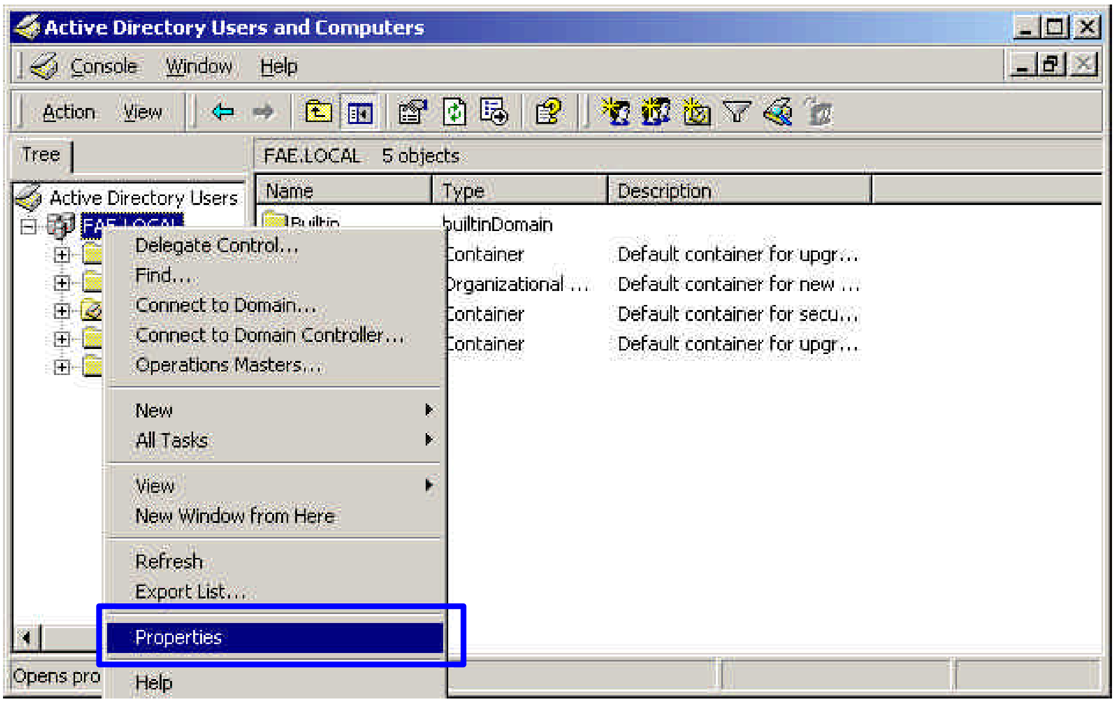


Select a certificate template to issue certificates

| | |
|---|---|
| User Signature Only | Secure Email, Clier |
| Smartcard User | Secure Email, Clier |
| Authenticated Session | Client Authenticatic |
| Smartcard Logon | Client Authenticatic |
| Code Signing | Code Signing |
| Trust List Signing | Microsoft Trust List |
| Enrollment Agent | Certificate Request |

11. Go to Start > Program > Administrative Tools > **Active Directory Users and Computers**.

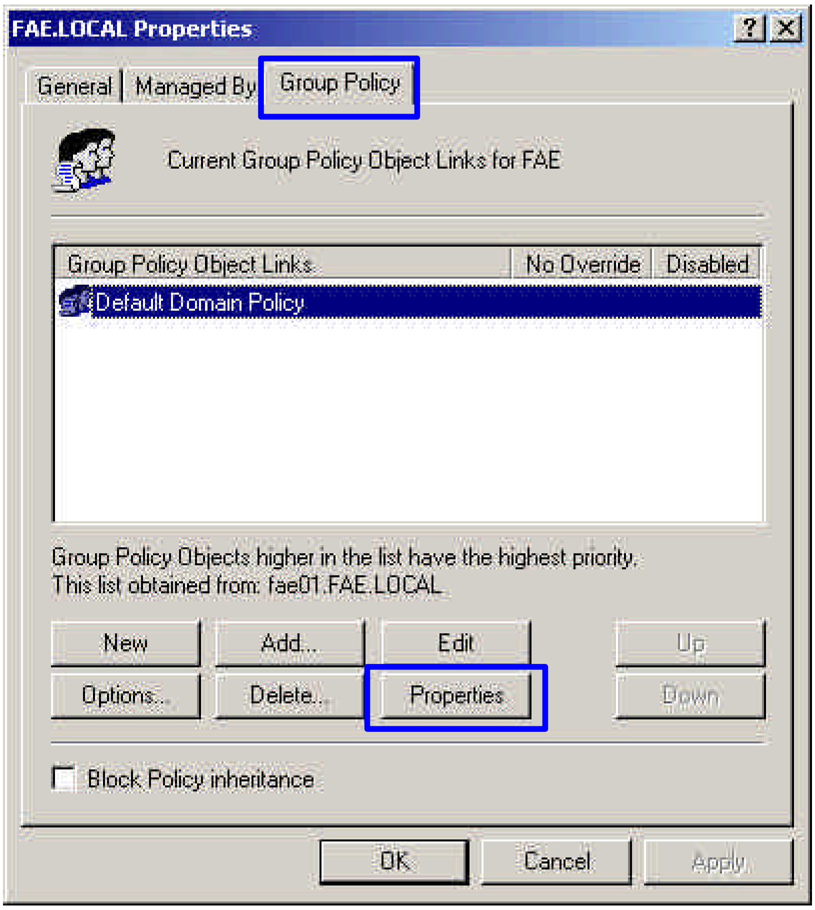
12. Right-click on domain, and select "**Properties**" to continue.



FAE.LOCAL 5 objects

| Name | Type | Description |
|---|---|---|
| Builtin | builtinDomain | |
| | Container | Default container for upgr... |
| | Organizational ... | Default container for new ... |
| | Container | Default container for secu... |
| | Container | Default container for upgr... |

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



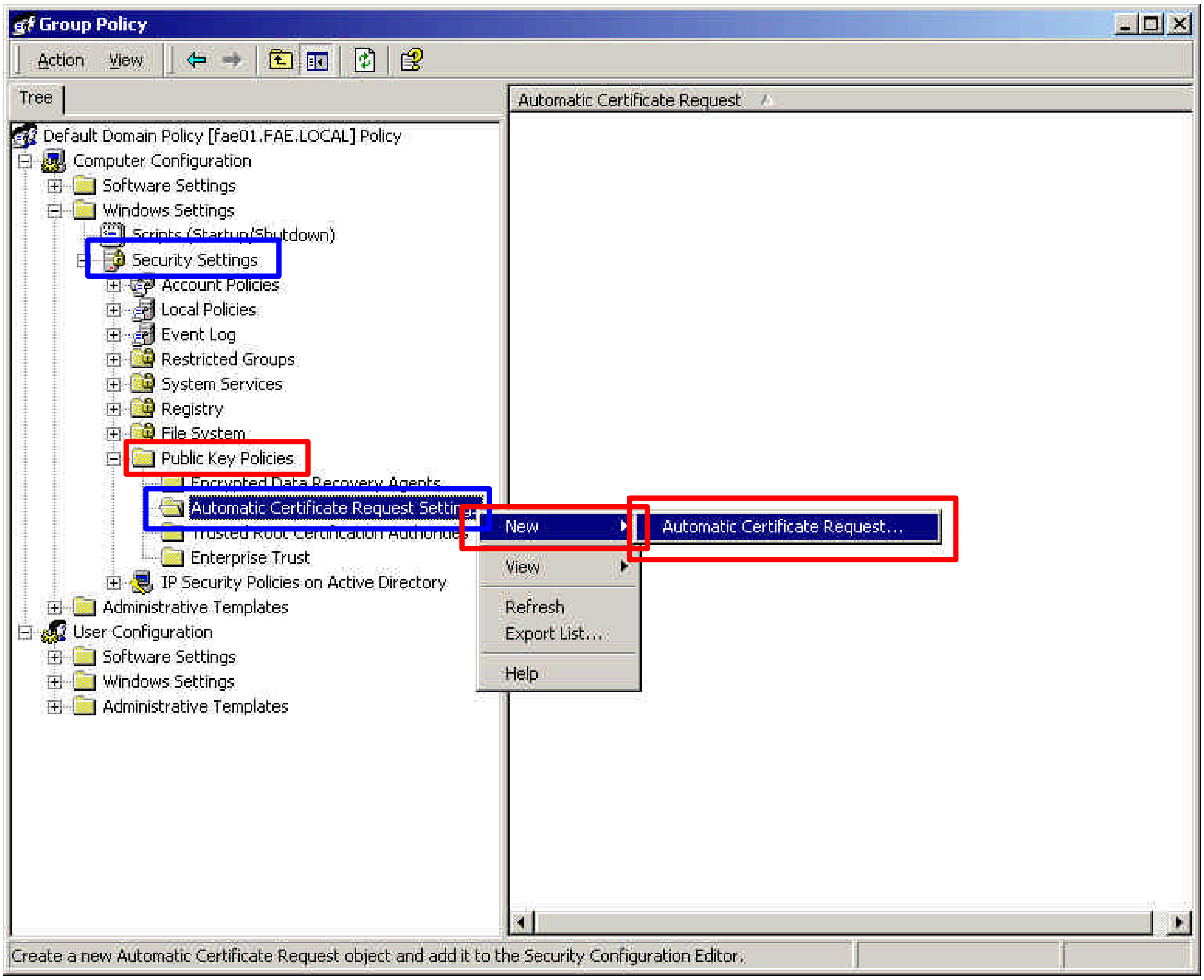
Current Group Policy Object Links for FAE

| Group Policy Object Links | No Override | Disabled |
|---|---|---|
| Default Domain Policy | | |

Group Policy Objects higher in the list have the highest priority.
This list obtained from: fae01.FAE.LOCAL

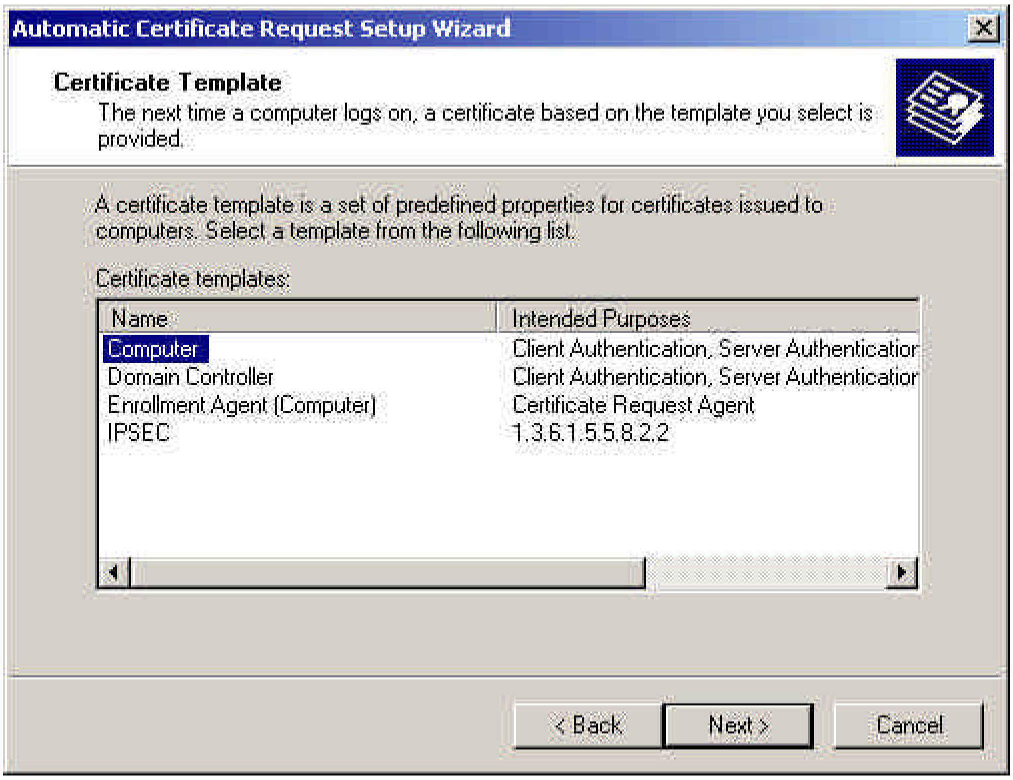
□ Block Policy inheritance

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 ...**”



Create a new Automatic Certificate Request object and add it to the Security Configuration Editor.

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



Automatic Certificate Request Setup Wizard

**Certificate Template**

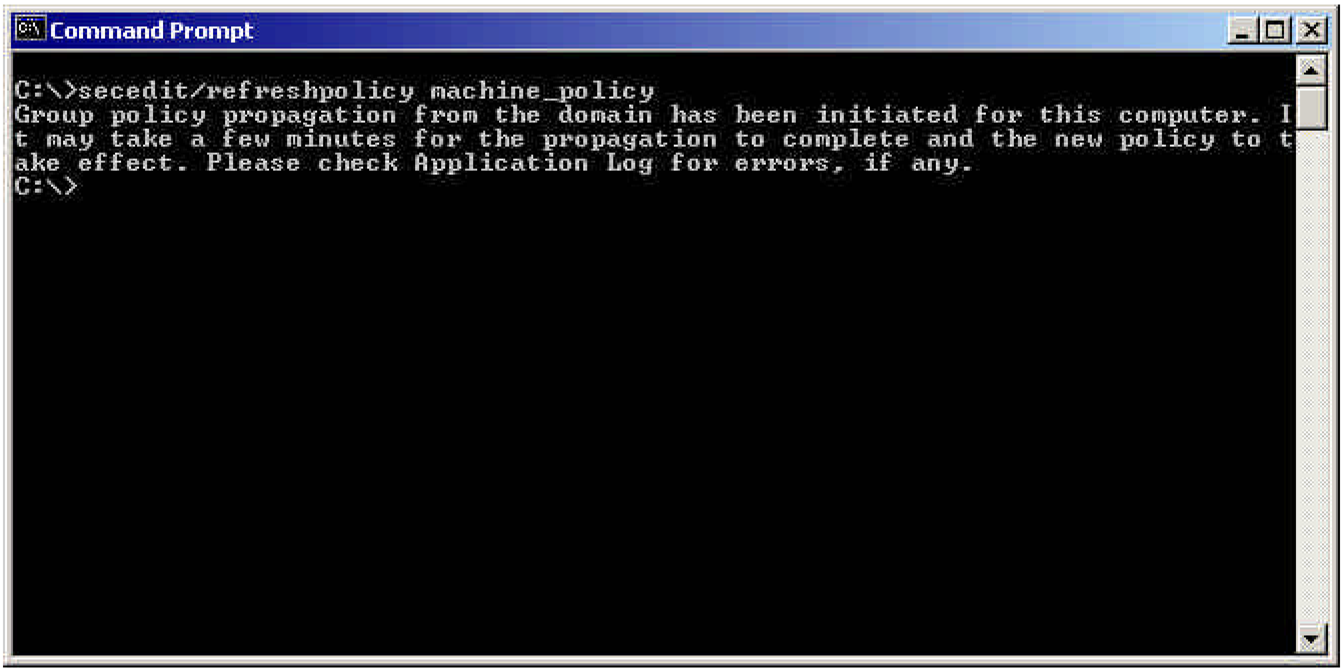
The next time a computer logs on, a certificate based on the template you select is provided.

A certificate template is a set of predefined properties for certificates issued to computers. Select a template from the following list.

Certificate templates:

| Name | Intended Purposes |
|---|---|
| Computer | Client Authentication, Server Authenticatior |
| Domain Controller | Client Authentication, Server Authenticatior |
| Enrollment Agent (Computer) | Certificate Request Agent |
| IPSEC | 1.3.6.1.5.5.8.2.2 |

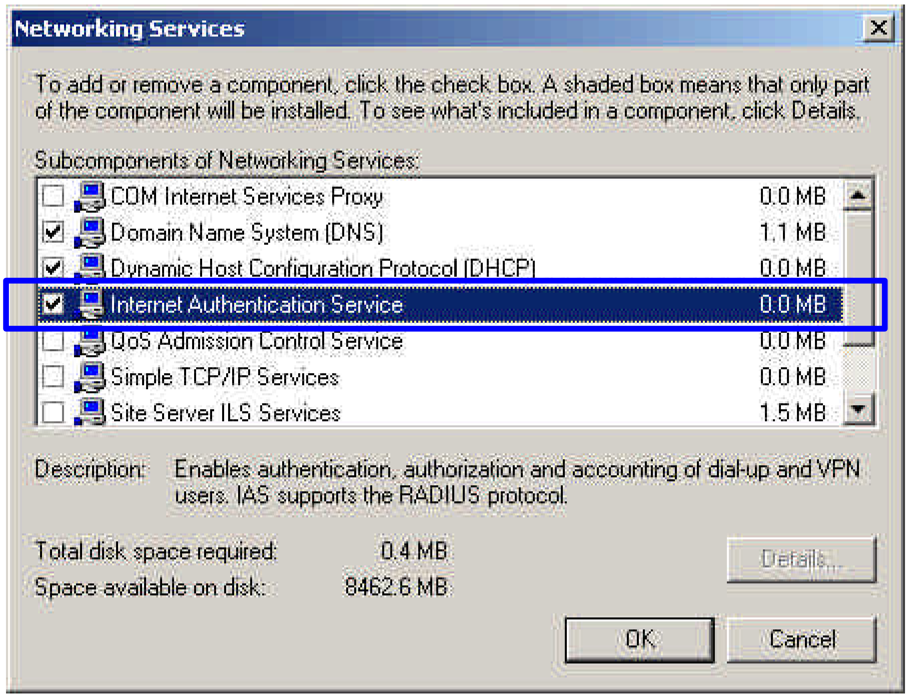
18. Click “**Finish**” to complete the Automatic Certificate Request Setup
19. Go to Start > **Run**, and type “**command**” and click “**Enter**” to open Command Prompt.
20. Type “secedit/refreshpolicy machine_policy” to refresh policy.



```
C:\>secedit/refreshpolicy machine_policy
Group policy propagation from the domain has been initiated for this computer. I
t may take a few minutes for the propagation to complete and the new policy to t
ake effect. Please check Application Log for errors, if any.
C:\>
```

### *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.



To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

| | | |
|---|---|---|
| □ | COM Internet Services Proxy | 0.0 MB |
| ☑ | Domain Name System (DNS) | 1.1 MB |
| ☑ | Dynamic Host Configuration Protocol (DHCP) | 0.0 MB |
| ☑ | Internet Authentication Service | 0.0 MB |
| □ | QoS Admission Control Service | 0.0 MB |
| □ | Simple TCP/IP Services | 0.0 MB |
| □ | Site Server ILS Services | 1.5 MB |

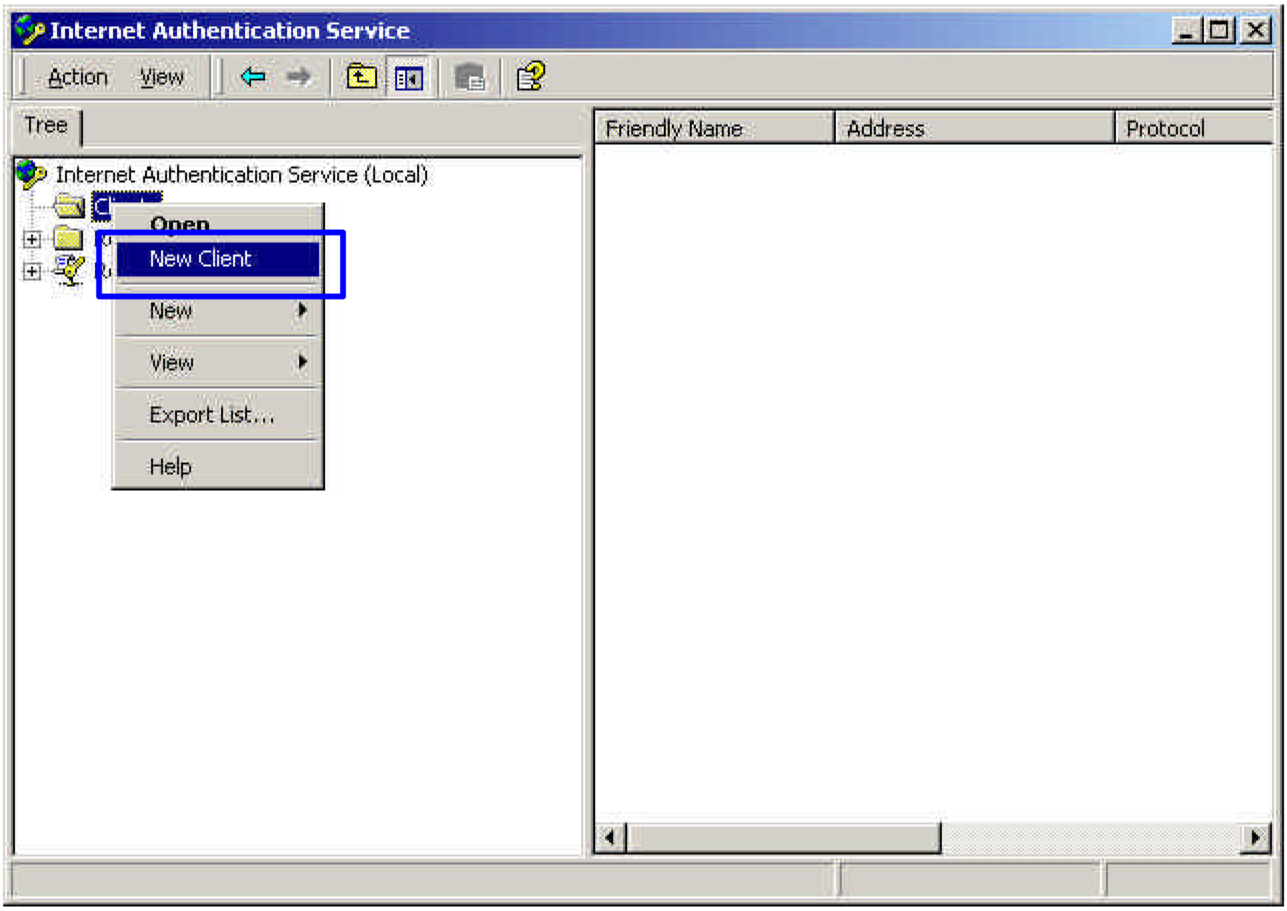
Description: Enables authentication, authorization and accounting of dial-up and VPN users. IAS supports the RADIUS protocol.

Total disk space required: 0.4 MB

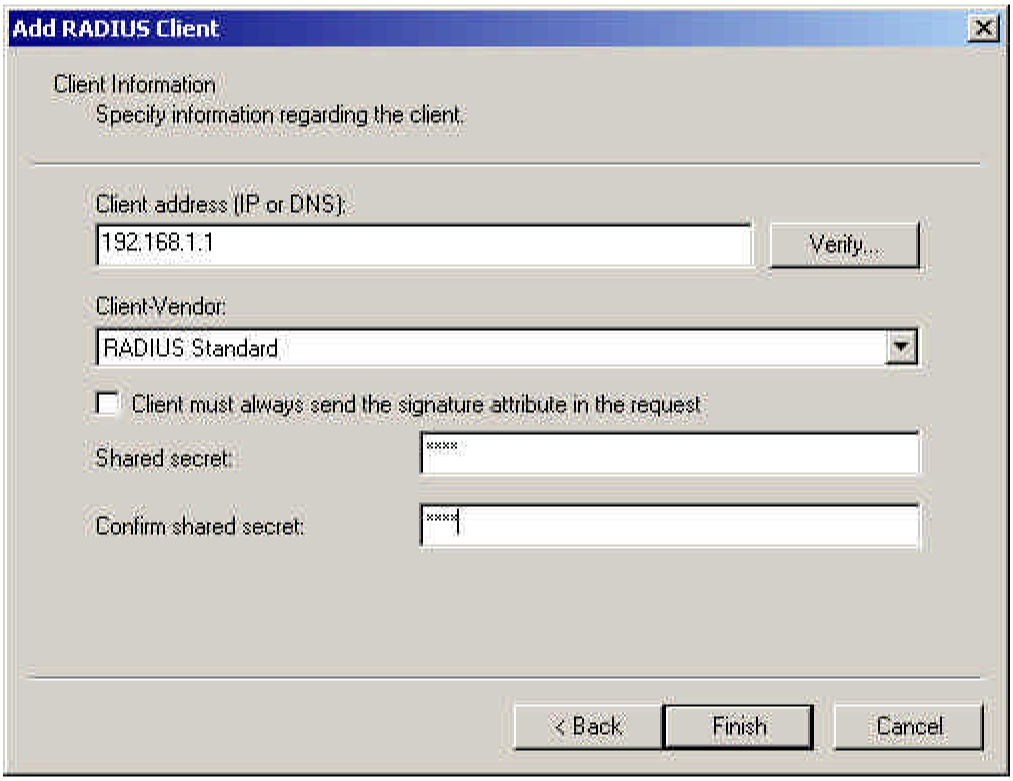
Space available on disk: 8462.6 MB

### *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.



Add RADIUS Client

Client Information
Specify information regarding the client.

Client address (IP or DNS):
192.168.1.1

Client-Vendor:
RADIUS Standard

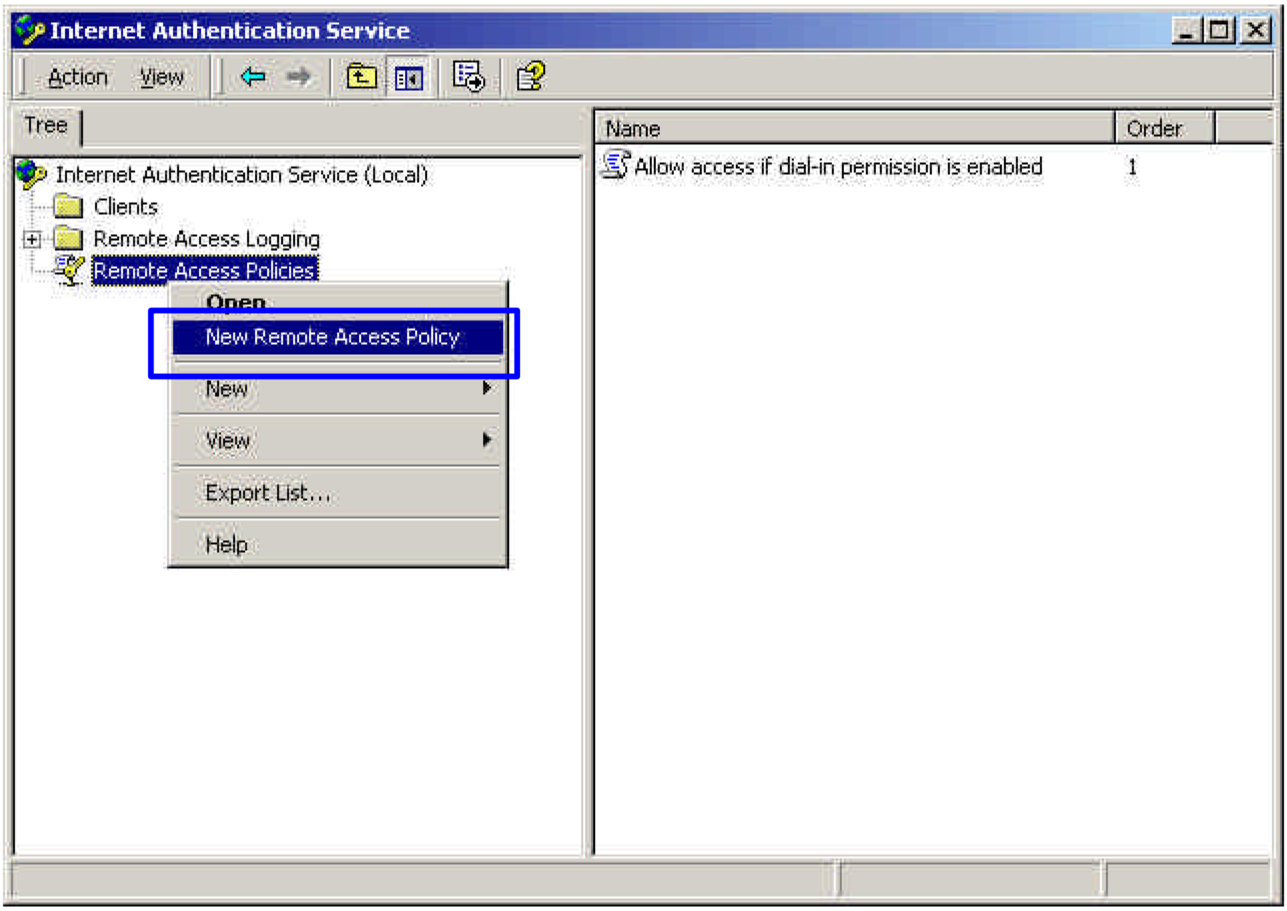
□ Client must always send the signature attribute in the request

Shared secret: ****

Confirm shared secret: ****

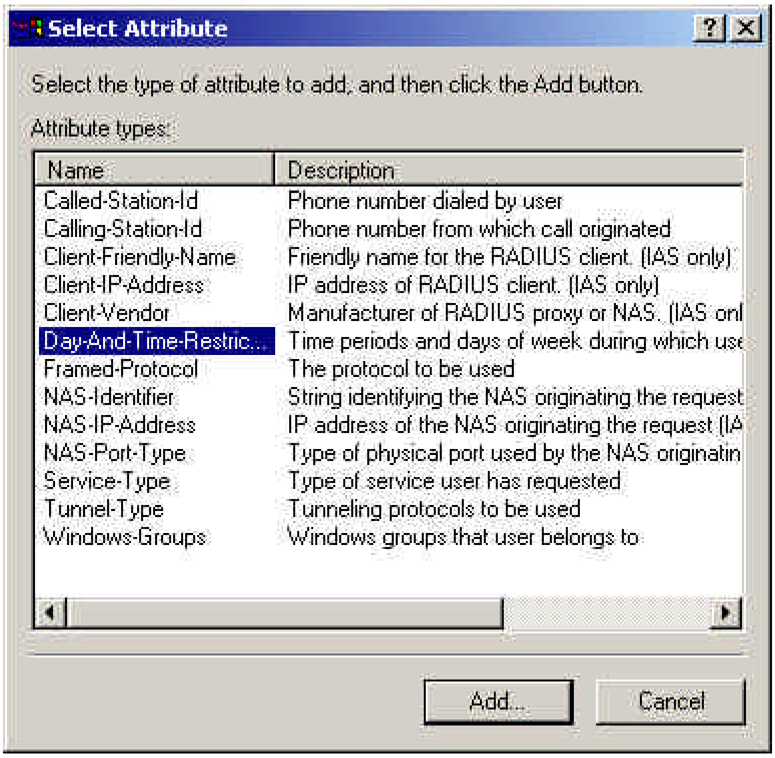
28. In the Internet Authentication Service, right-click “**Remote Access Policies**”

29. Select “New Remote Access Policy”.



| Name | Order |
|---|---|
| Allow access if dial-in permission is enabled | 1 |

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

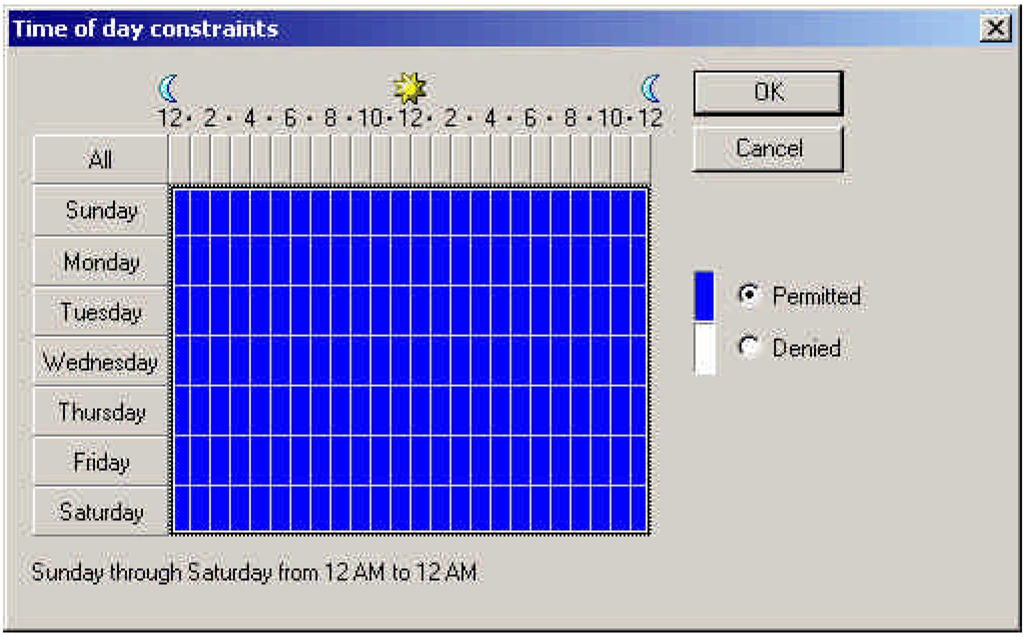


Select the type of attribute to add, and then click the Add button.

Attribute types:

| Name | Description |
|---|---|
| Called-Station-Id | Phone number dialed by user |
| Calling-Station-Id | Phone number from which call originated |
| Client-Friendly-Name | Friendly name for the RADIUS client. (IAS only) |
| Client-IP-Address | IP address of RADIUS client. (IAS only) |
| Client-Vendor | Manufacturer of RADIUS proxy or NAS. (IAS onl |
| Day-And-Time-Restric... | Time periods and days of week during which use |
| Framed-Protocol | The protocol to be used |
| NAS-Identifier | String identifying the NAS originating the request |
| NAS-IP-Address | IP address of the NAS originating the request (IA |
| NAS-Port-Type | Type of physical port used by the NAS originatin |
| Service-Type | Type of service user has requested |
| Tunnel-Type | Tunneling protocols to be used |
| Windows-Groups | Windows groups that user belongs to |

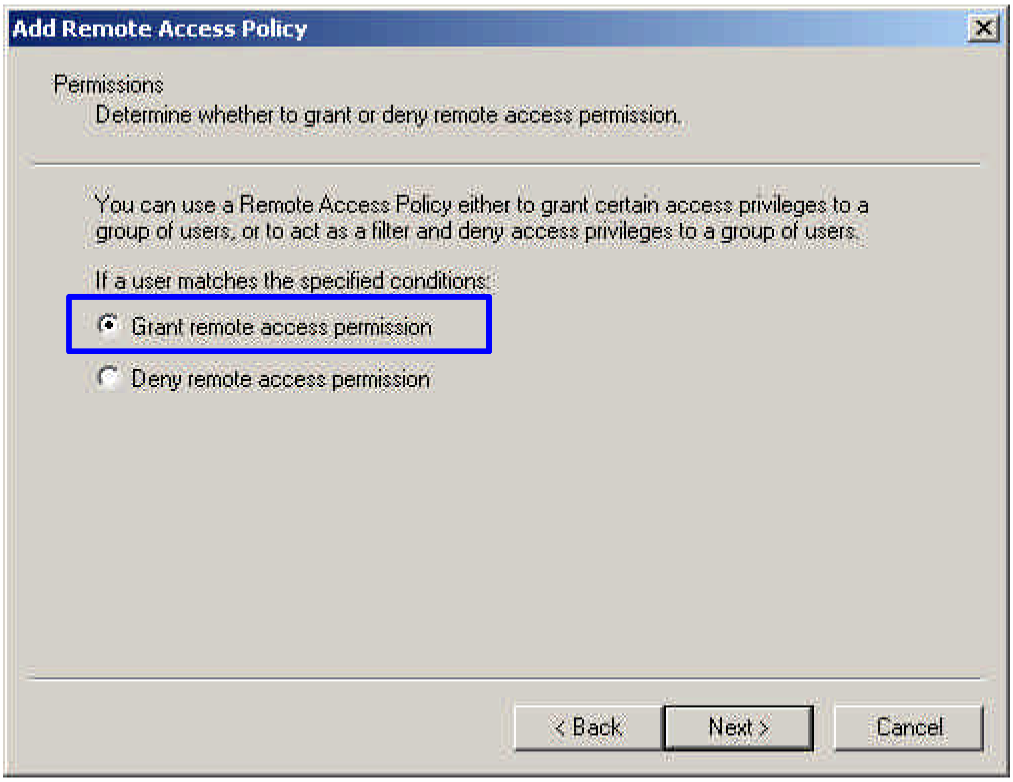
31. Unless you want to specify the active duration for 802.1x authentication, click “**OK**” to accept to have 802.1x authentication enabled at all times.



● Permitted
○ Denied

Sunday through Saturday from 12 AM to 12 AM

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



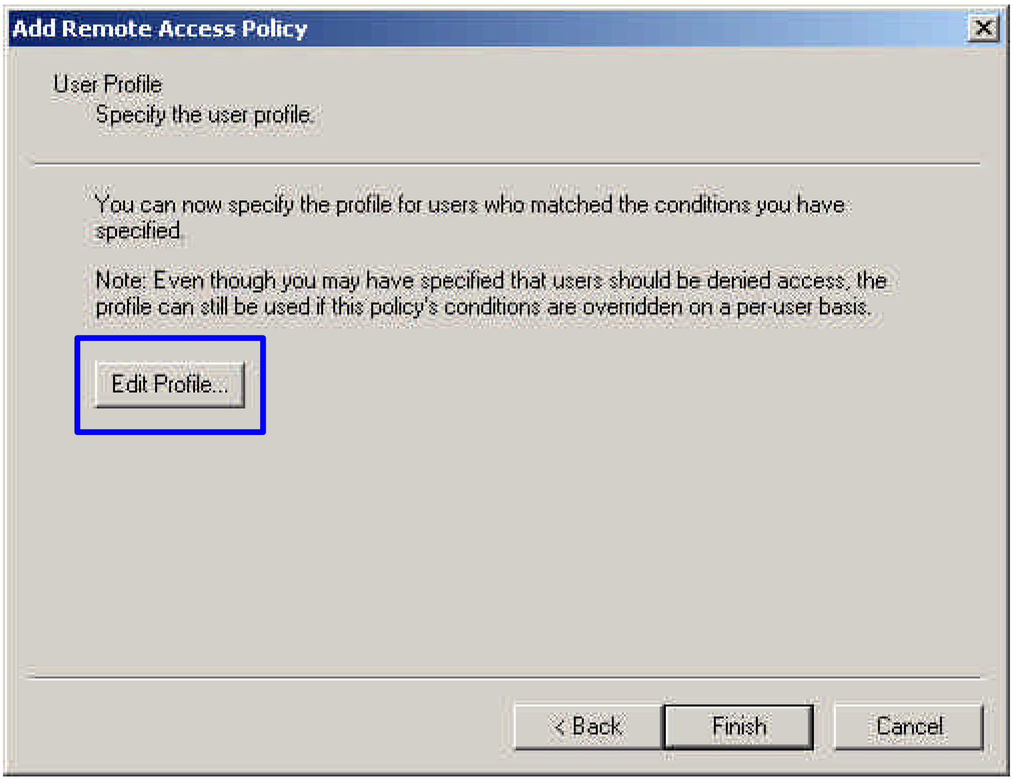
Permissions
Determine whether to grant or deny remote access permission.

You can use a Remote Access Policy either to grant certain access privileges to a group of users, or to act as a filter and deny access privileges to a group of users.

If a user matches the specified conditions:

● Grant remote access permission
○ Deny remote access permission

33. Click “Edit Profile” to open up



Add Remote Access Policy

User Profile

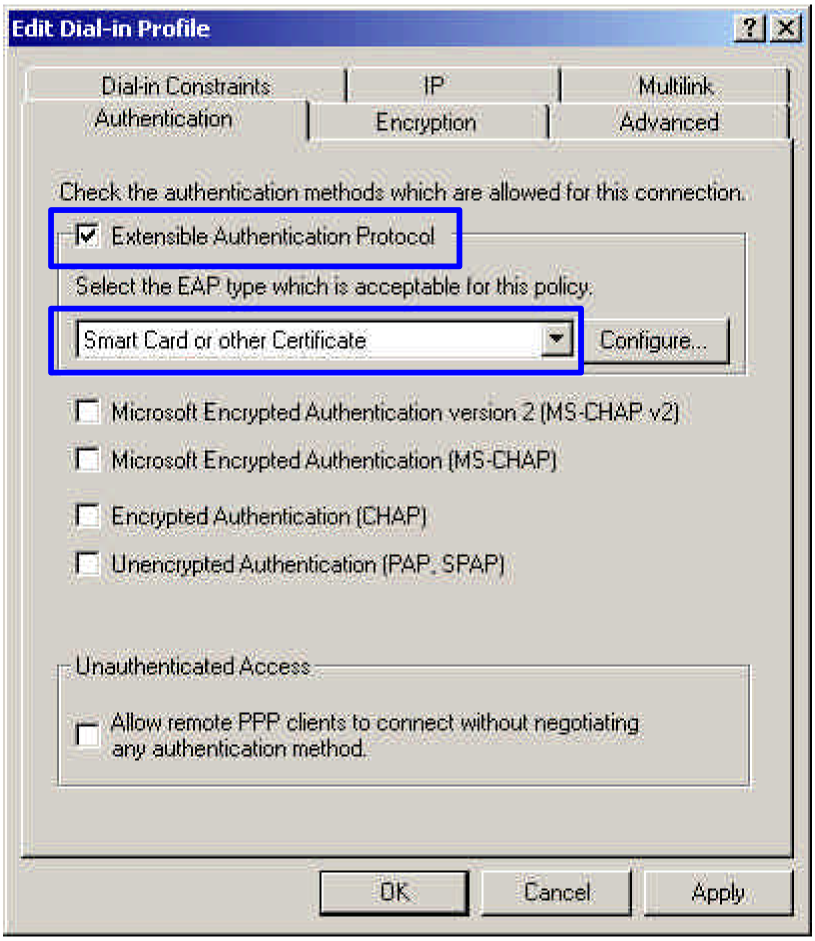
Specify the user profile.

You can now specify the profile for users who matched the conditions you have specified.

Note: Even though you may have specified that users should be denied access, the profile can still be used if this policy's conditions are overridden on a per-user basis.

***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



Check the authentication methods which are allowed for this connection.

☑ Extensible Authentication Protocol

Select the EAP type which is acceptable for this policy:

Smart Card or other Certificate

□ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

□ Microsoft Encrypted Authentication (MS-CHAP)

□ Encrypted Authentication (CHAP)

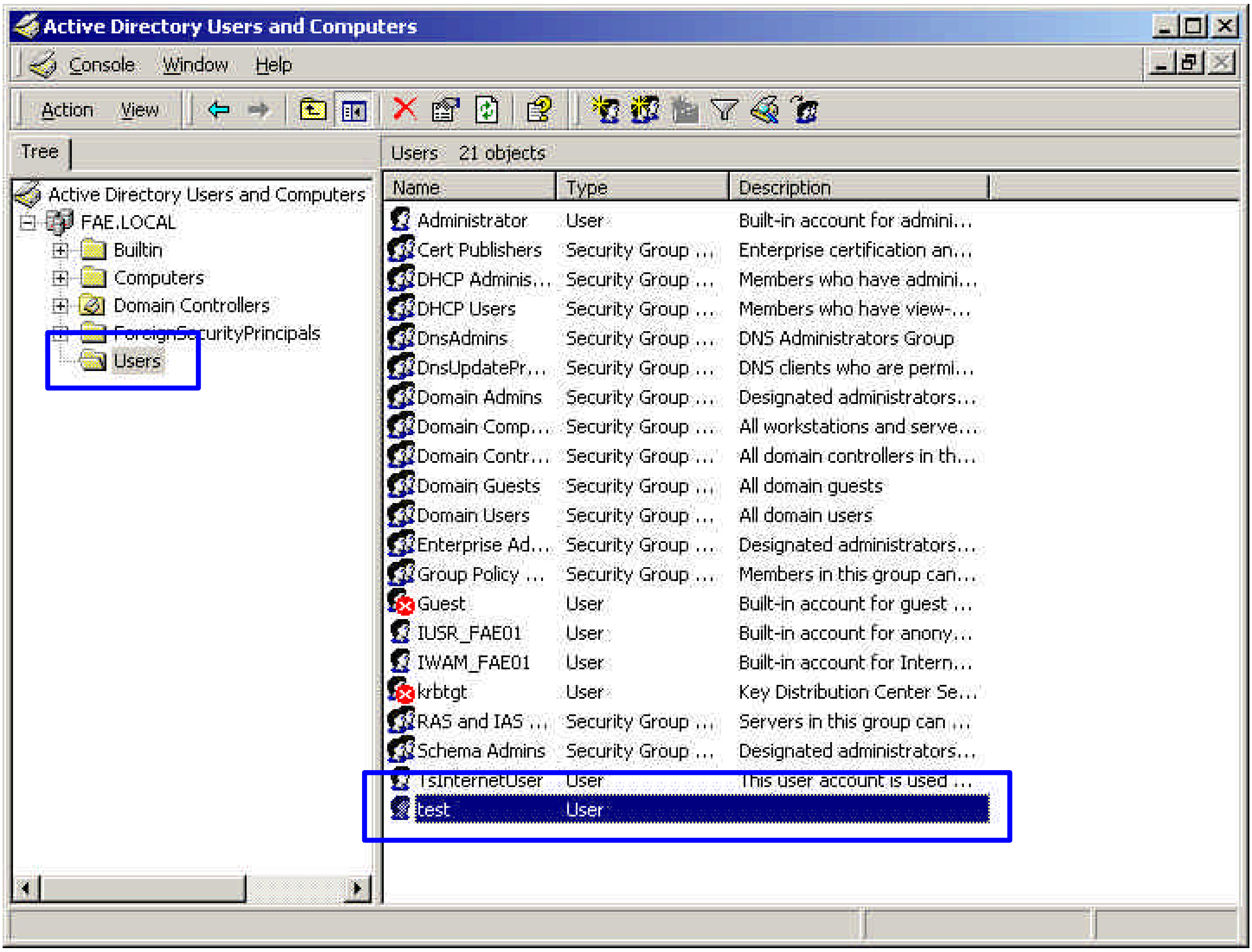
□ Unencrypted Authentication (PAP, SPAP)

Unauthenticated Access

□ Allow remote PPP clients to connect without negotiating any authentication method.

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.

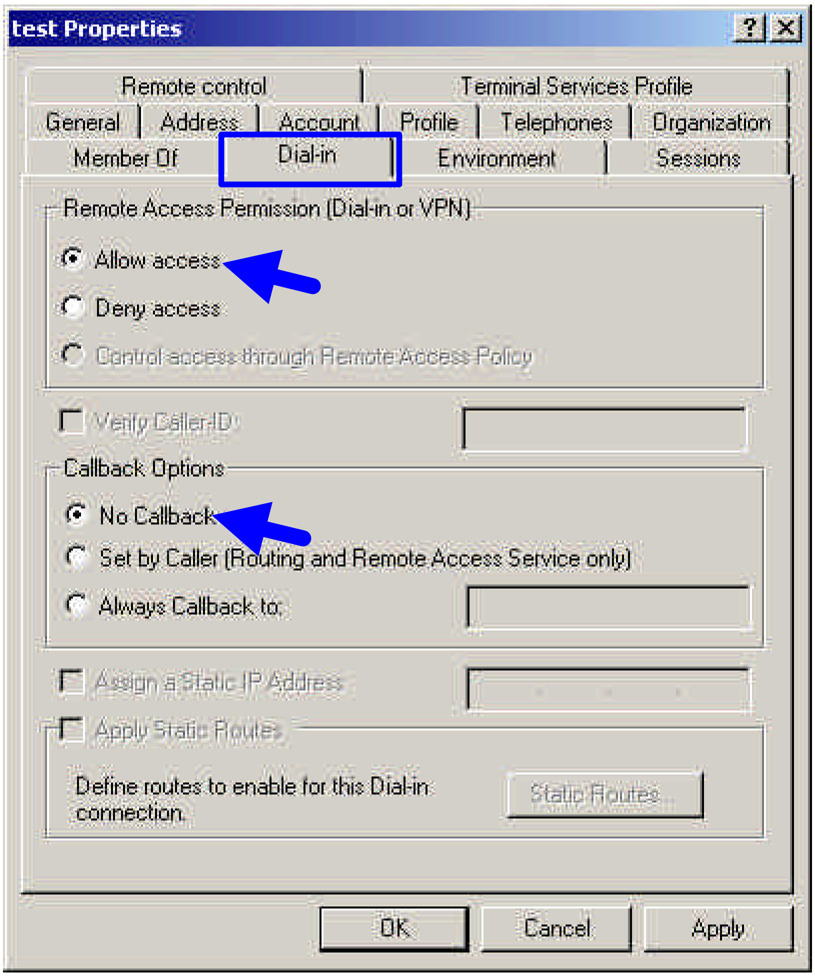

Active Directory Users and Computers
Console
Window
Help
Action
View
Tree
Active Directory Users and Computers
FAE.LOCAL
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users

Users 21 objects

| Name | Type | Description |
|---|---|---|
| Administrator | User | Built-in account for admini… |
| Cert Publishers | Security Group … | Enterprise certification an… |
| DHCP Adminis… | Security Group … | Members who have admini… |
| DHCP Users | Security Group … | Members who have view-… |
| 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 … |
| IUSR_FAE01 | User | Built-in account for anony… |
| IWAM_FAE01 | User | Built-in account for Intern… |
| krbtgt | User | Key Distribution Center Se… |
| RAS and IAS … | Security Group … | Servers in this group can … |
| Schema Admins | Security Group … | Designated administrators… |
| TsInternetUser | User | This user account is used … |
| test | User | |

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.



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:

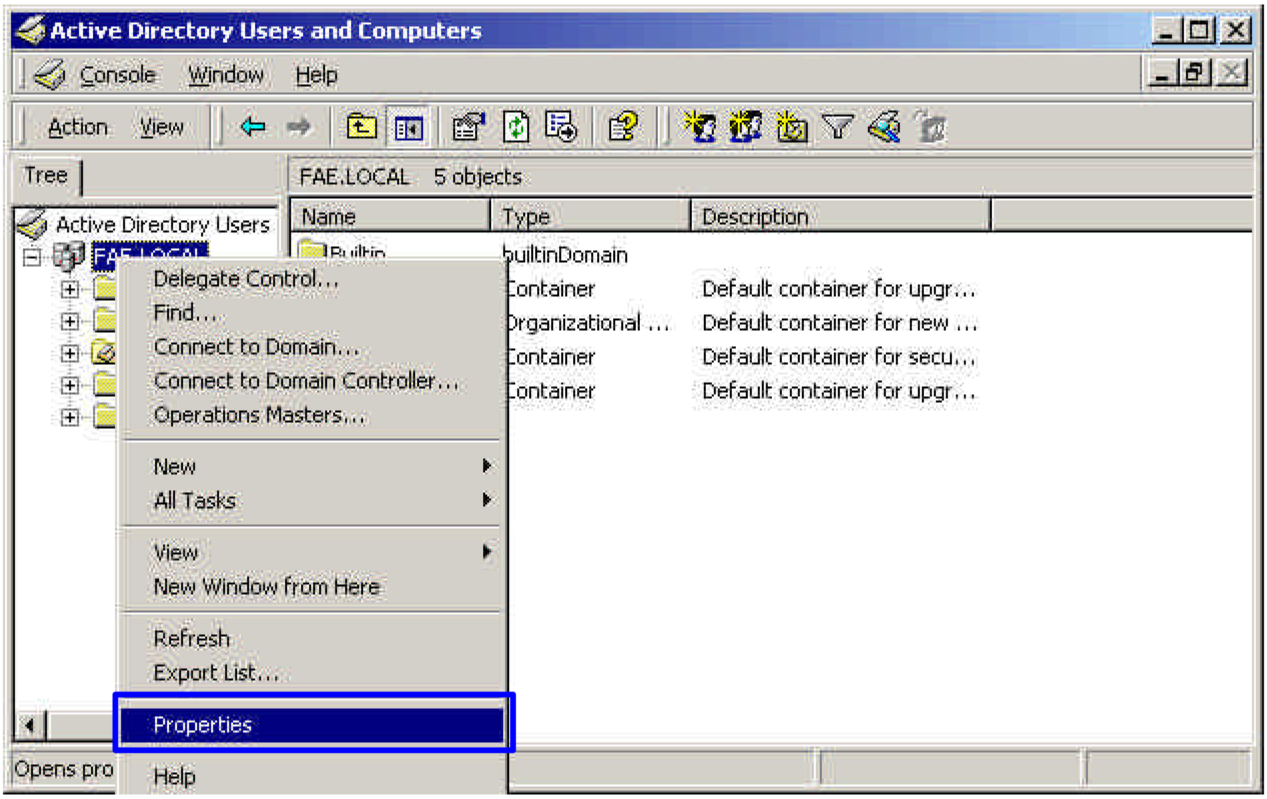
□ Assign a Static IP Address

□ Apply Static Routes

Define routes to enable for this Dial-in connection.

*For MD5 Authentication (Steps 39 ~ 54)*

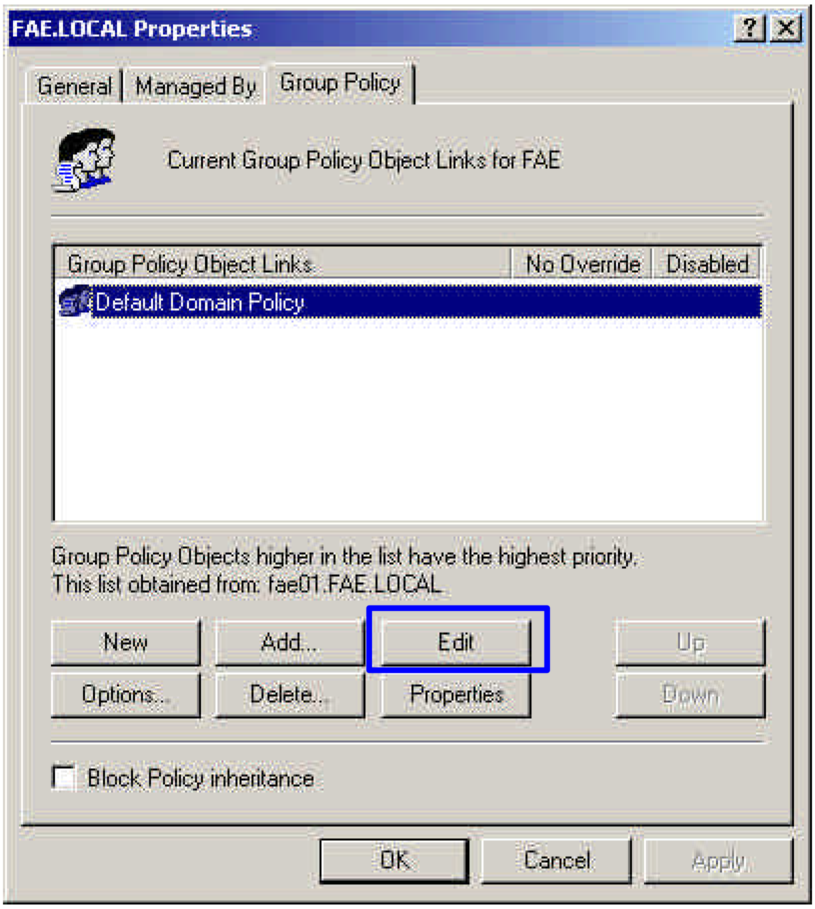
39. Go to Start > Program > Administrative Tools > **Active Directory Users and Computers.**
40. Right click on the domain, and select "**Properties**"



FAE.LOCAL 5 objects

| Name | Type | Description |
|---|---|---|
| Builtin | builtinDomain | |
| | ontainer | Default container for upgr... |
| | rganizational ... | Default container for new ... |
| | ontainer | Default container for secu... |
| | ontainer | Default container for upgr... |

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



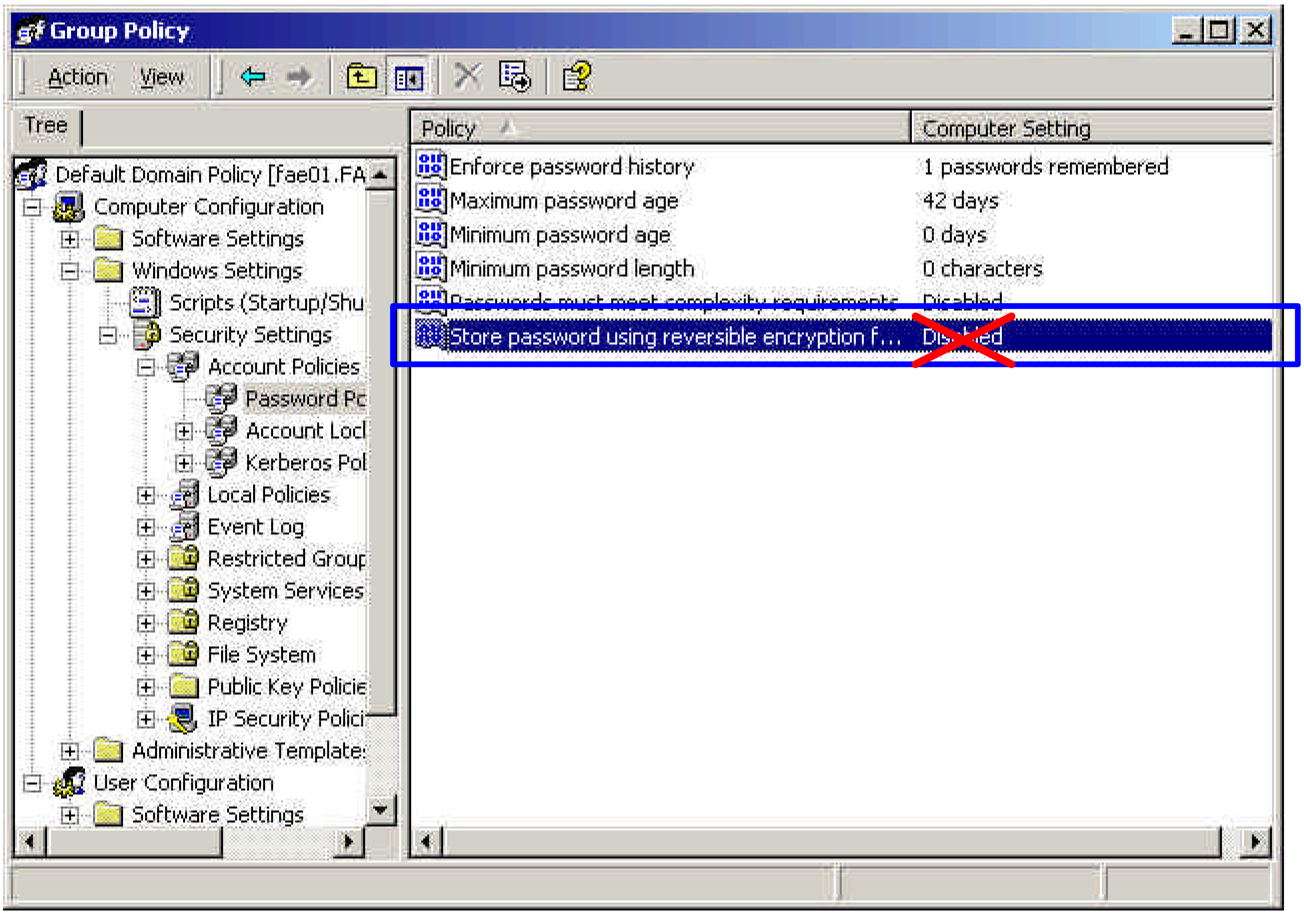
Current Group Policy Object Links for FAE

| Group Policy Object Links | No Override | Disabled |
|---|---|---|
| Default Domain Policy | | |

Group Policy Objects higher in the list have the highest priority.
This list obtained from: fae01.FAE.LOCAL

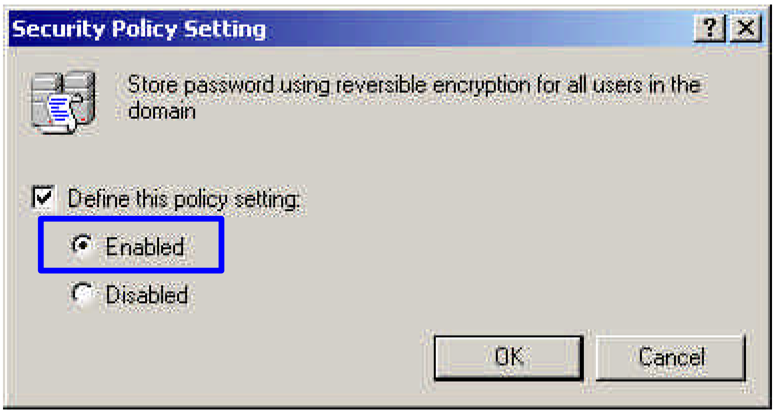
□ Block Policy inheritance

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



| Policy | Computer Setting |
|---|---|
| Enforce password history | 1 passwords remembered |
| Maximum password age | 42 days |
| Minimum password age | 0 days |
| Minimum password length | 0 characters |
| Passwords must meet complexity requirements | Disabled |
| Store password using reversible encryption f... | Disabled |

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



Store password using reversible encryption for all users in the domain

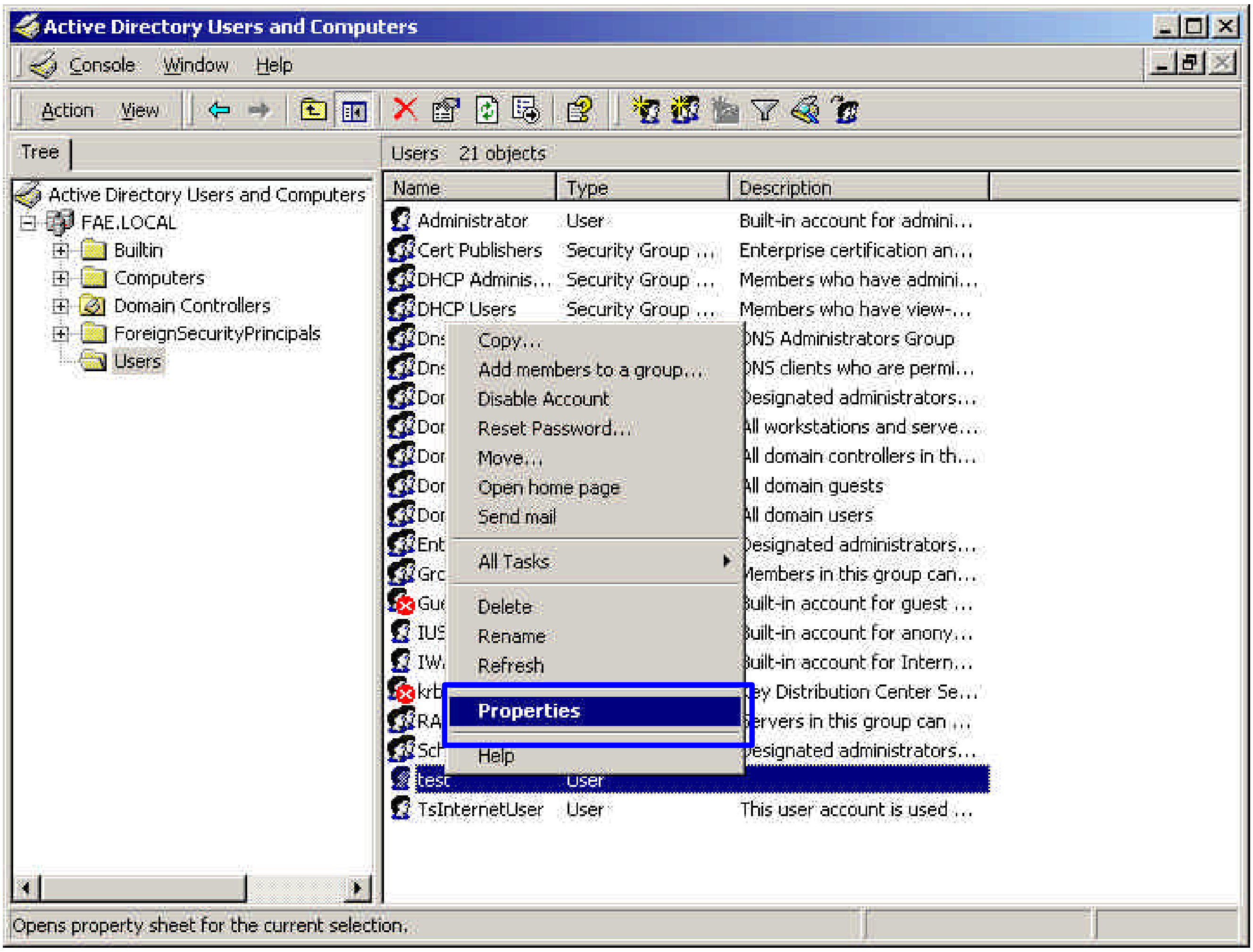
☑ Define this policy setting:

● Enabled

○ Disabled

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**"

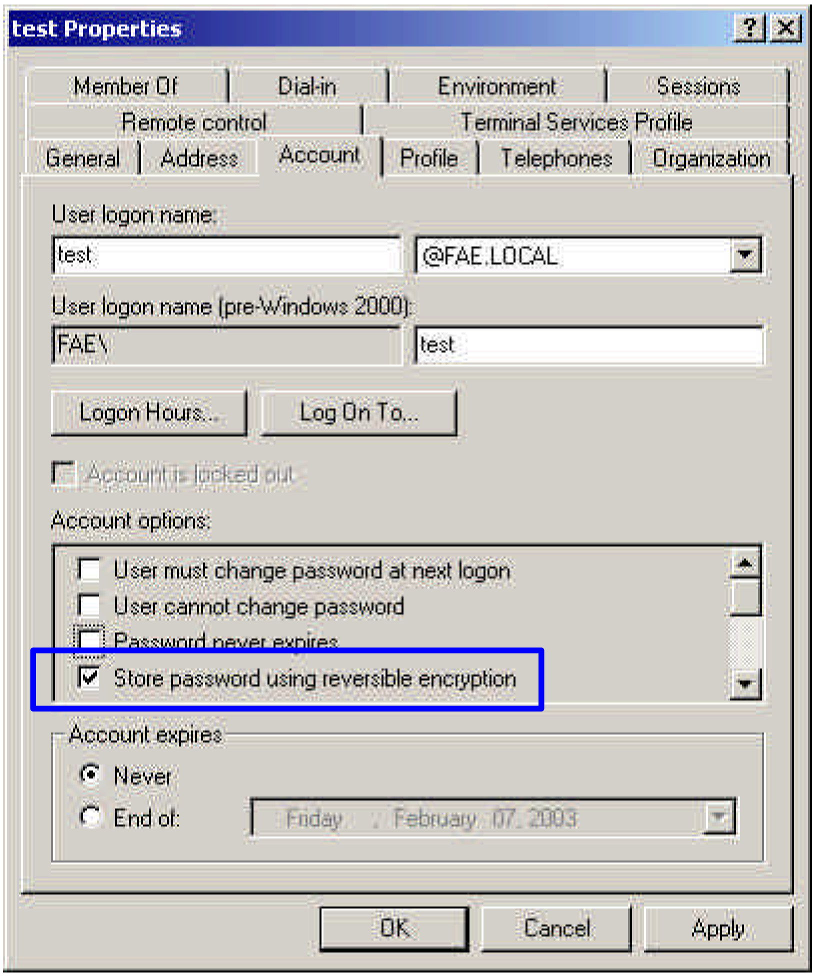


| Name | Type | Description |
|---|---|---|
| Administrator | User | Built-in account for admini... |
| Cert Publishers | Security Group ... | Enterprise certification an... |
| DHCP Adminis... | Security Group ... | Members who have admini... |
| DHCP Users | Security Group ... | Members who have view-... |
| Dns | | )NS Administrators Group |
| Dns | | )NS clients who are permi... |
| Dor | | )esignated administrators... |
| Dor | | ll workstations and serve... |
| Dor | | ll domain controllers in th... |
| Dor | | ll domain guests |
| Dor | | ll domain users |
| Ent | | )esignated administrators... |
| Grc | | Members in this group can... |
| Gue | | Built-in account for guest ... |
| IUS | | Built-in account for anony... |
| IW. | | Built-in account for Intern... |
| krb | | ey Distribution Center Se... |
| RA | | ervers in this group can ... |
| Sch | | )esignated administrators... |
| test | User | |
| TsInternetUser | User | This user account is used ... |

Opens property sheet for the current selection.

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

47. Click “**OK**” to continue.



test Properties

User logon name: test @FAE.LOCAL

User logon name (pre-Windows 2000): FAE\ test

□ Account is locked out

Account options:

□ User must change password at next logon
□ User cannot change password
□ Password never expires
☑ Store password using reversible encryption

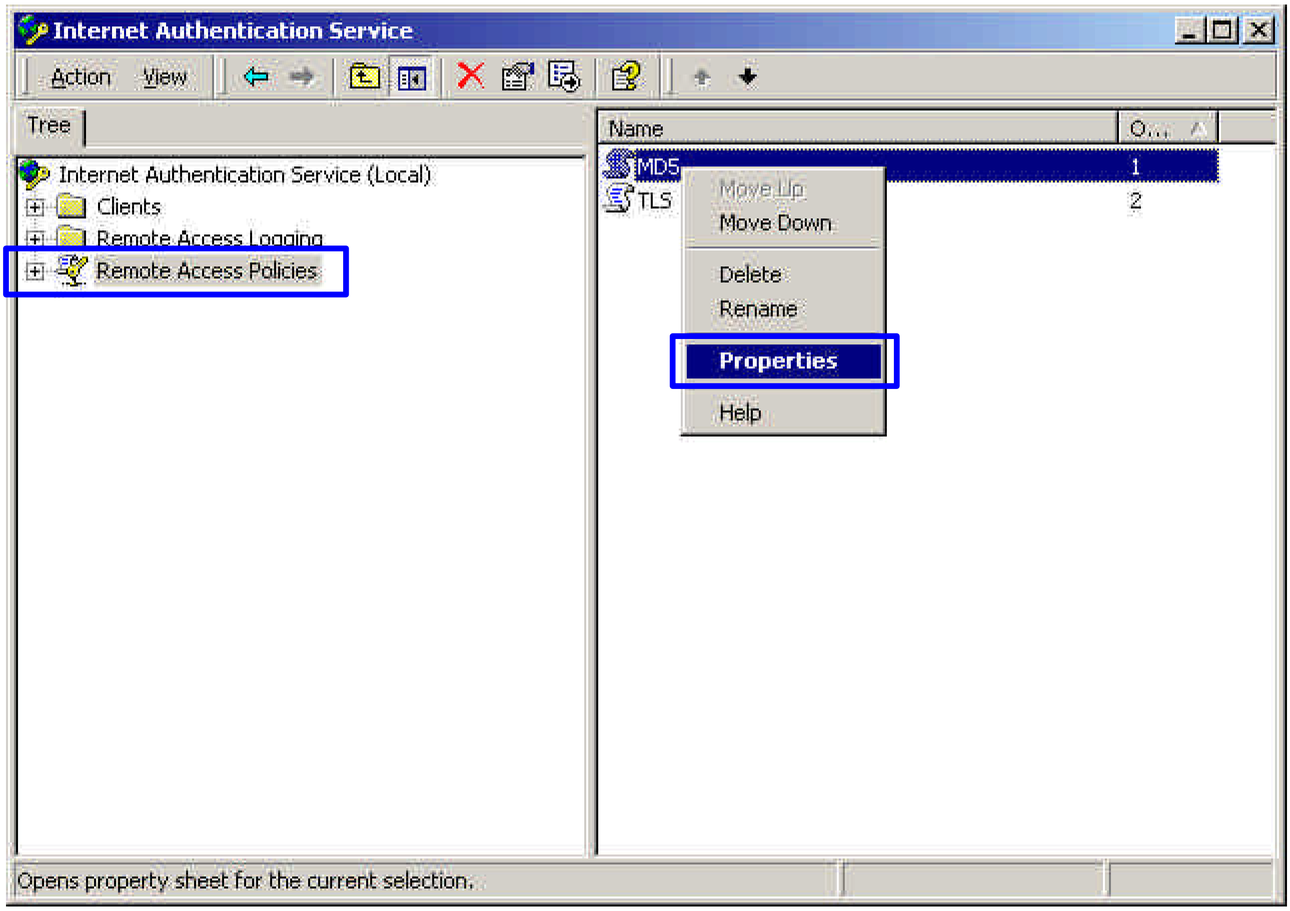
Account expires
● Never
○ End of: Friday , February 07, 2003

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**"

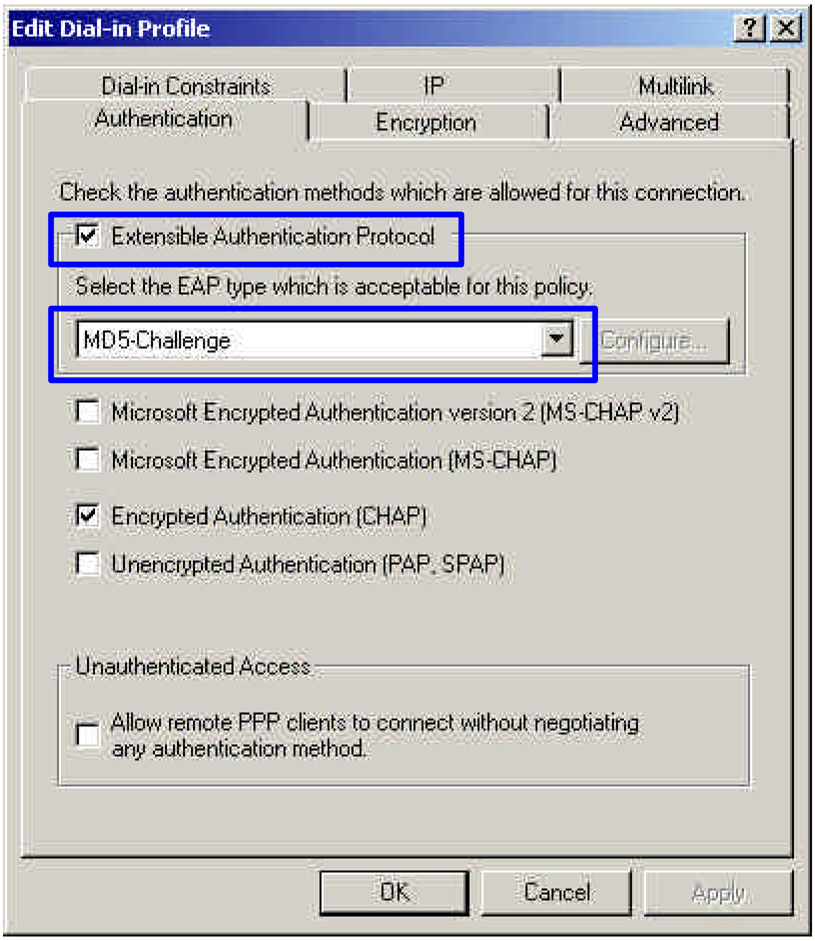


Opens property sheet for the current selection.

52. Go to “**Authentication**” tab

53. Enable “**Extensible Authentication Protocol**”

54. Select “**MD5-Challenge**” for EAP type.



Edit Dial-in Profile

Check the authentication methods which are allowed for this connection.

☑ Extensible Authentication Protocol

Select the EAP type which is acceptable for this policy.

MD5-Challenge

□ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

□ Microsoft Encrypted Authentication (MS-CHAP)

☑ Encrypted Authentication (CHAP)

□ Unencrypted Authentication (PAP, SPAP)

Unauthenticated Access

□ Allow remote PPP clients to connect without negotiating any authentication method.

# 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 **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers, 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** ? **R**equest **T**o **S**end. 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 @25ºC ± 5ºC) | |
| **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 | |