

How To Set Up Wireless Network Security

Part 1: WEP

Part 2: WPA-PSK

Part 3-1: RADIUS Server Installation

Part 3-2: 802.1x-TLS

Part 3-3: WPA

You can secure your wireless connection using one of the methods described below. Choose the one most suitable for your network. For simple networks WEP or WPA-PSK are most suitable, complex networks with installed RADIUS services can use WPA.

Part 1: WEP

Step1: Setting up Access Point's WEP encryption key.

1. Log into the Access Point using your WEB browser (e.g. Internet Explorer). Go to Wireless configuration page (Home > Wireless).

Select the WEP option (Enable).

2. Select the "Key Mode" (ASCII or Hex).

ASCII (American Standard Code for Information Interchange): the standard for assigning numerical values to the set of letters in the Roman alphabet and typographic characters.

HEX (Hexadecimal): numbers from 0 to 9 and letters from A to F.

3. Select WEP Key length.

64 bit: 5 ASCII or 10 Hex charcters

128 bit: 13 ASCII or 26 Hex characters

4. Select default key.

There are 4 WEP keys that can be used. Default key is the key number 1.

Select key 1, other three keys can be ignored.

5. Press "Apply" to complete your settings.

The screenshot shows the configuration page for a D-Link DWL-2000AP. The page is titled "AirPlus Xtreme G High-Speed 2.4GHz Wireless Access Point". The "Advanced" tab is selected. The "Wireless Settings" section is visible, showing the following configuration:

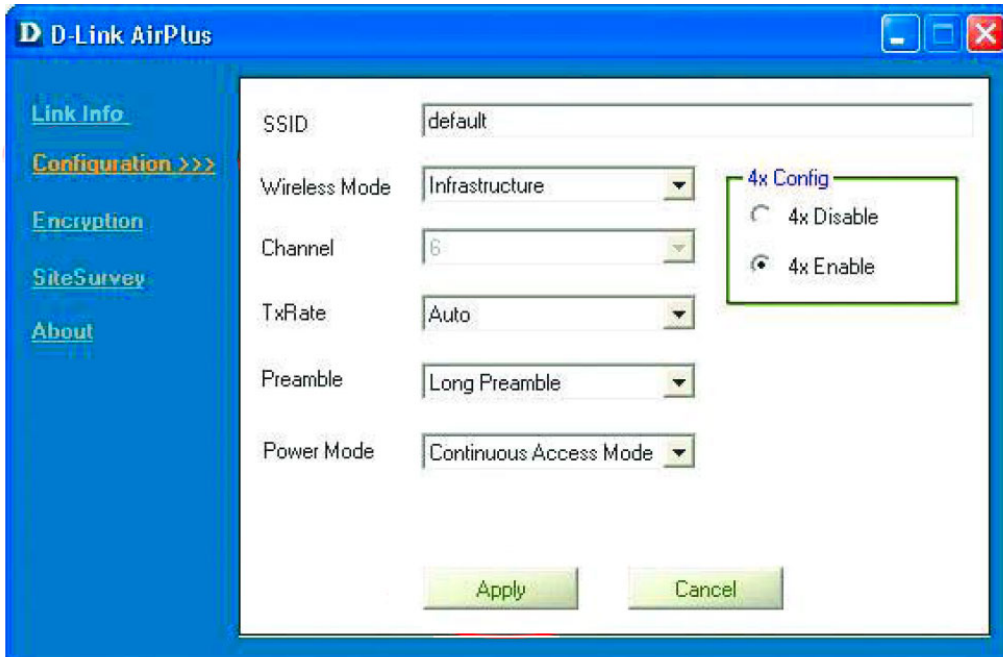
- AP Name: DWL-2000AP
- SSID: feet
- Channel: 6
- Authentication: Open System Shared Key WPA WPA-PSK
- WEP: Enabled Disabled
- WEP Encryption: 64Bit
- WEP Mode: HEX
- Key1: 1111111111
- Key2: 0000000000
- Key3: 0000000000
- Key4: 0000000000

At the bottom right, there are three buttons: "Apply" (with a green checkmark icon), "Cancel" (with a red X icon), and "Help" (with a red plus icon).

Step 2: Setting up Workstation's WEP Key.

2a. If you are using D-Link Wireless Utility to configure your D-Link Wireless Card:

1. Open the D-Link AirPlus wireless utility by double-clicking on the bar graph icon and select Encryption.
2. Put a check in the "Data Encryption" box and select "Shared Authentication" in the auth. mode menu. Select 64, or 128 encryption for the key length. Under key 1 type in the Hex or ASCII encryption key that was entered into the wireless router/access point.



2b. If you are using Windows XP to configure your wireless card:

1. Right-click "My Network Places" on your desktop and click "Properties" (or go to Start > Control Panel > Network)
2. Select your Wireless LAN Card, right click on the icon and select "Properties". Click on "Wireless Network" tab.
3. Select the Access Point which you going to connect to and click "Configuration" on the right.
4. Under "Wireless Network Properties" tick "Data encryption (WEP Enabled)". Uncheck "The key is provided for me automatically".
5. Select "key index" which is the default key for your station (Note: in some versions of Windows the indexes are from 0 to 3 which are mapped to keys 1 to 4).
6. Key in your WEP Key value into "Network Key" (exactly the same as the one entered on your Access Point).
8. Press "OK" to finish your workstation's WEP settings.

Wireless Network Properties



Network name (SSID):

Wireless network key (WEP)

This network requires a key for the following:

- Data encryption (WEP enabled)
- Network Authentication (Shared mode)

Network key:

Key format: ▼

Key length: ▼

Key index (advanced): ▲ ▼

The key is provided for me automatically

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

OK

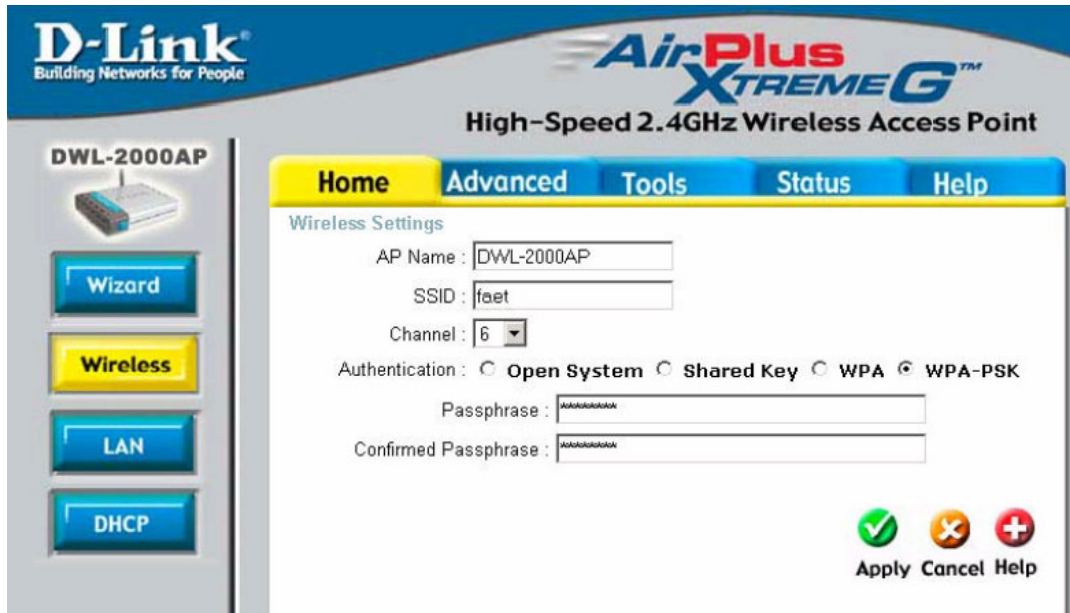
Cancel

Part 2: WPA-PSK

Since WPA-PSK standard is an extension of WEP key technology, its configuration is very similar to the WEP key configuration:

Step1: Setting up Access Point's WPA-PSK

1. Log into the Access Point using your WEB browser (e.g. Internet Explorer). Go to Wireless configuration page (Home > Wireless). Select the WPA-PSK option (Enable).
2. Key in your security code (no less than eight characters)
3. Press "Apply" to complete Access Point's configuration.



Step2: Setting up Workstation's WPA-PSK

1. We are using Windows XP as an example.
2. Right-click "My Network Places" on your desktop and click "Properties" (or go to Start > Control Panel > Network)
3. Select your Wireless LAN Card, right click on the icon and select "Properties". Click on "Wireless Network" tab.
4. Select the Access Point which you going to connect to and click "Configuration" on the right.
5. Under "Network Authentication" select "WPA-PSK". Under "Data encryption" select "TKIP"
7. Key in your "Network Key" which should be same you entered on your Access Point
8. Press "OK" to finish your workstation's WPA-PSK settings.

Wireless network properties [?] [X]

Association | **Authentication**

Network name (SSID):

Wireless network key

This network requires a key for the following:

Network Authentication: ▼

Data encryption: ▼

Network key:

Confirm network key:

Key index (advanced): ▼

The key is provided for me automatically

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

OK Cancel

Part 3: 802.1x and WPA

Part 3-1: RADIUS Server Installation

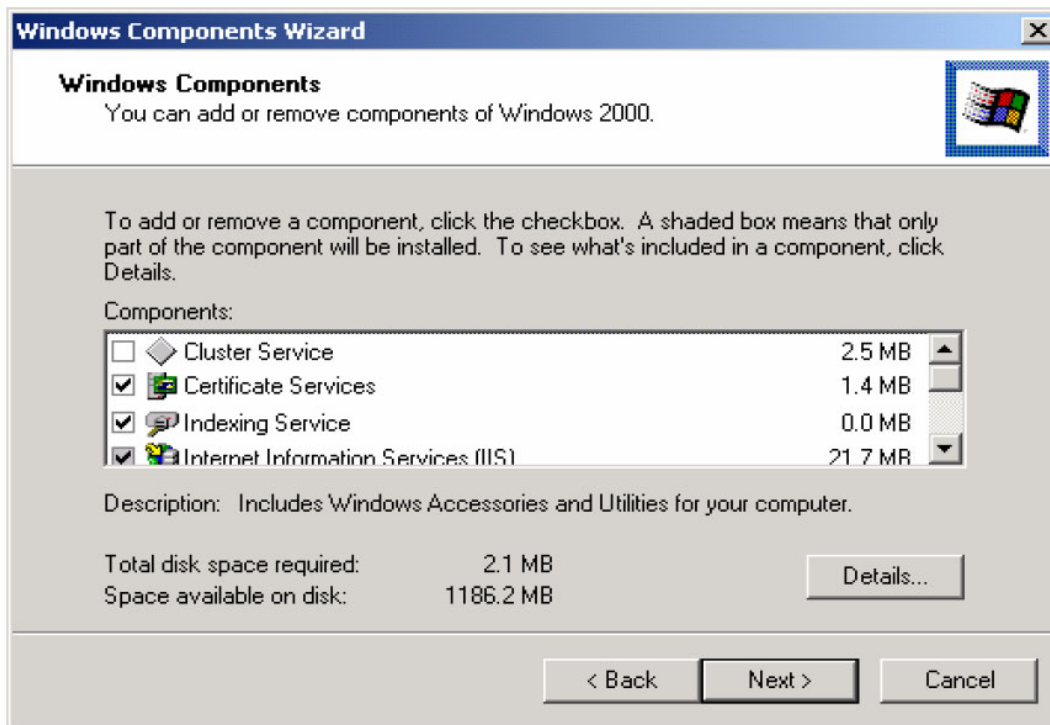
WPA implementation requires RADIUS services running on your network. We will use RADIUS Server running on Windows 2000 and 802.1x-TLS as an example.

Setting up RADIUS Server:

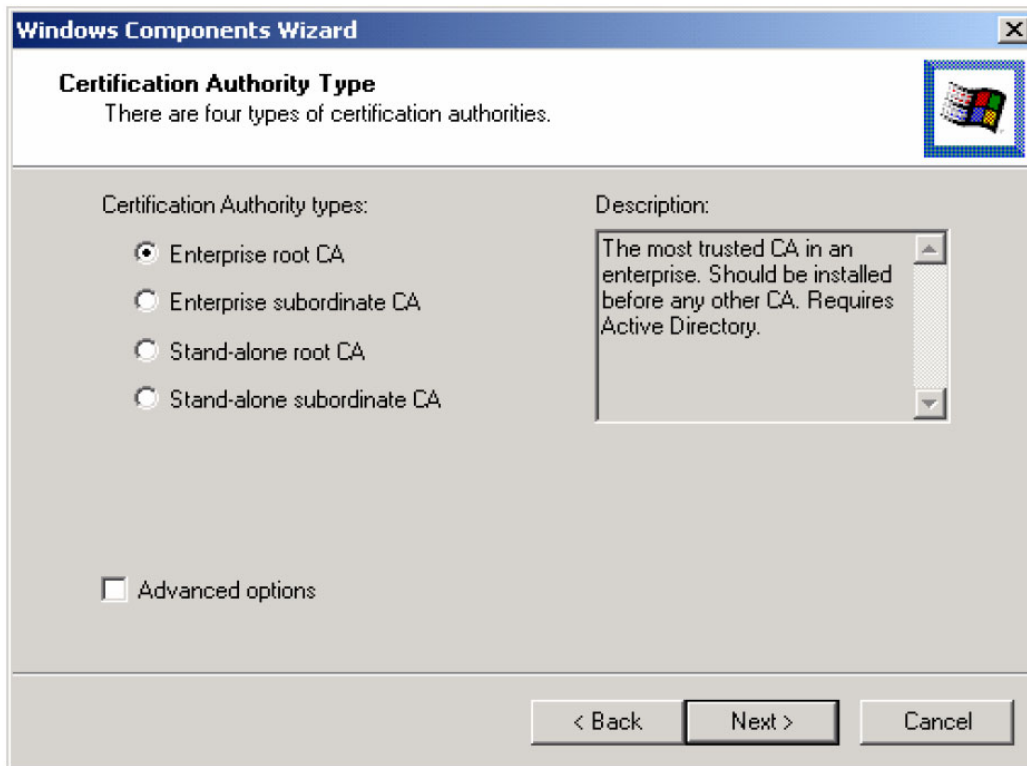
- Windows 2000 Server with Active Directory configuration.
- The server is set as Domain controller with DHCP/DNS enabled.
- For 802.1x, Windows 2000 requires Service Pack 3 or later.
- For WPA, Windows 2000 requires Service Pack 4 or later.

Step 1: Certificate Authority Installation

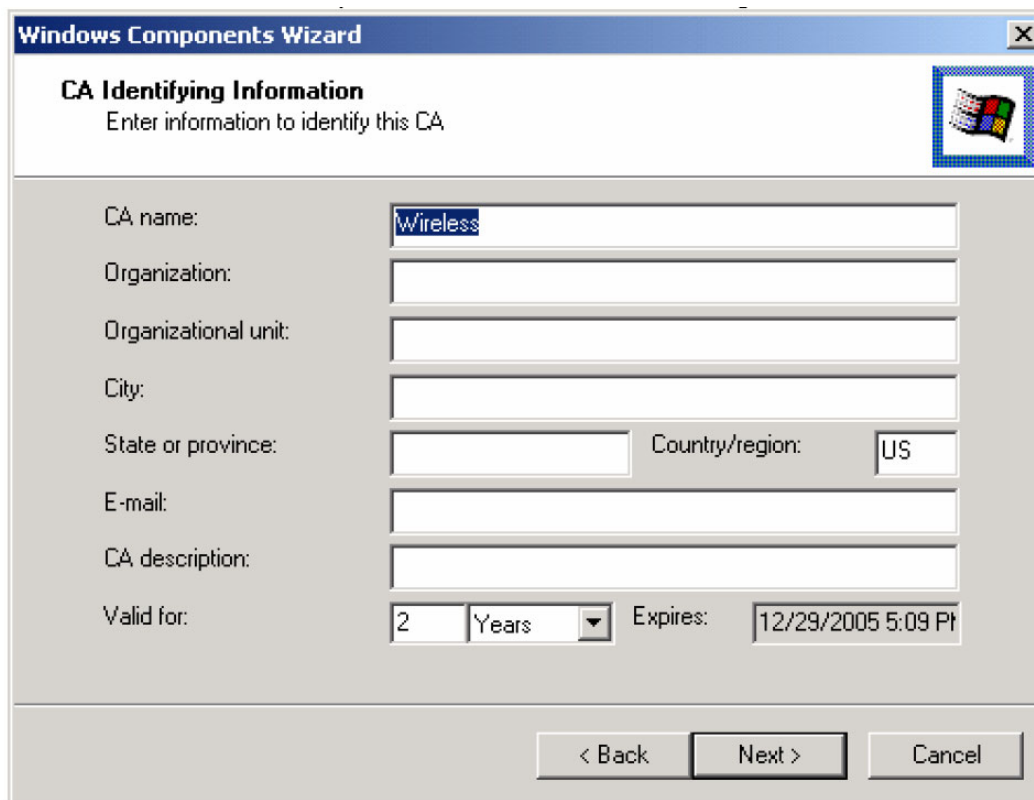
1. Logon into your Windows 2000 server as Administrator.
2. Go to Start > Control Panel > Add or Remove Programs.
3. Select "Add or remove Windows Components".
4. Tick "Certificate Services" and press "Next".



5. Click "Enterprise root CA" press "Next".



6. Put a CA name to identify this Certificate Service and press "Next".



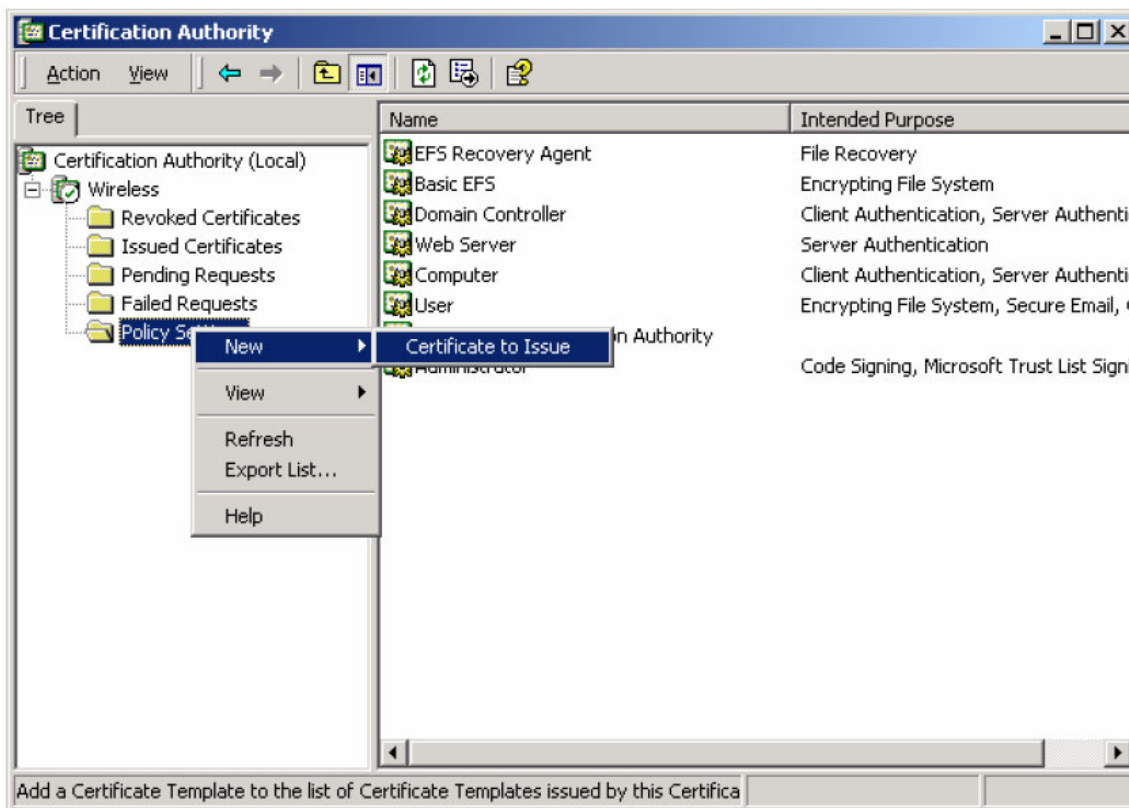
7. Specify data storage location, database and recode files and Press "Next".

8. You will see "Computer processing Internet information service. You need to stop this service to continue". Press "Yes" to continue.

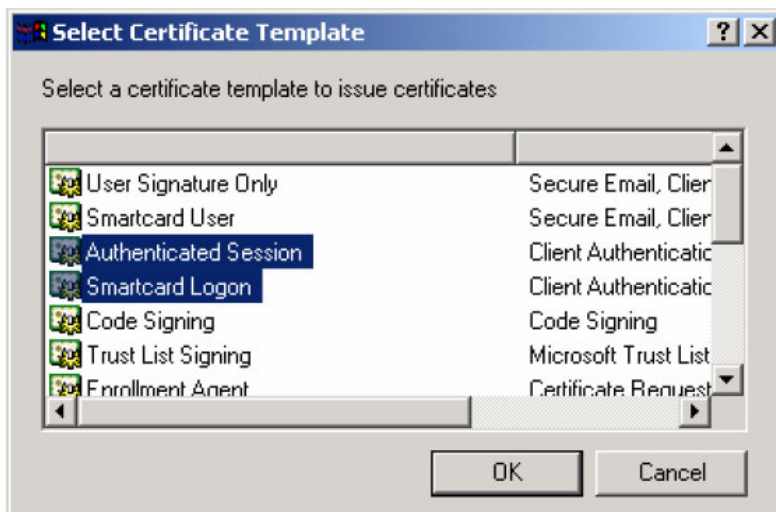
9. Press "Complete" to finish the Wizard.

Step 2: Certificate Authority Configuration

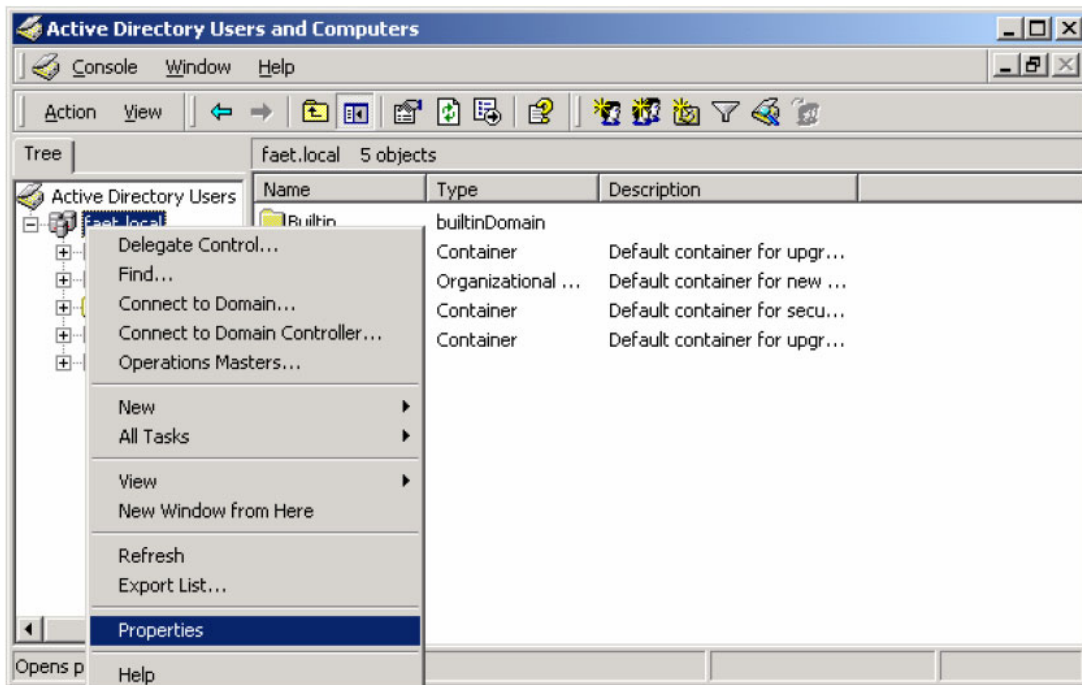
1. Go to Start>Program files> System administrative tools>Certificate Authority.
2. Open “Wireless” (the one you added into your system), right-click on the “Policy Setting” and select “New”.
3. Select “Certificate to Issue”



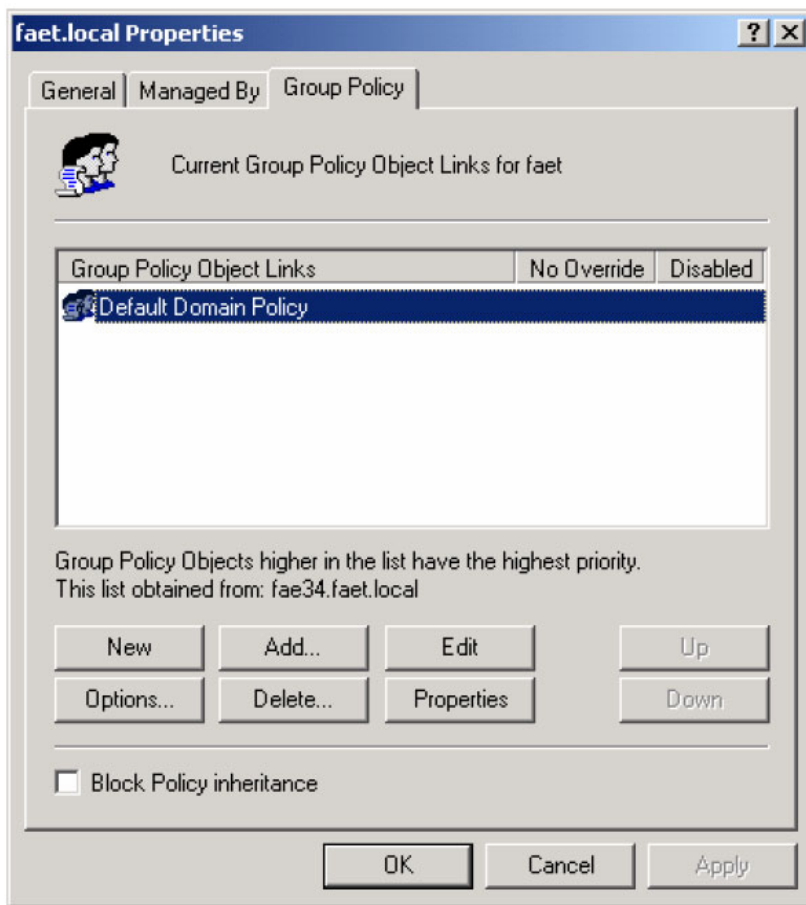
4. Select two Certificates: "Authenticated Session" and "Smartcard Logon" by holding down Ctrl key. Press "OK" to continue.



5. Go to Start> Program> System Administrative Tools> Active Directory Users and Computers.
6. Right Click on your Domain and click "Properties".



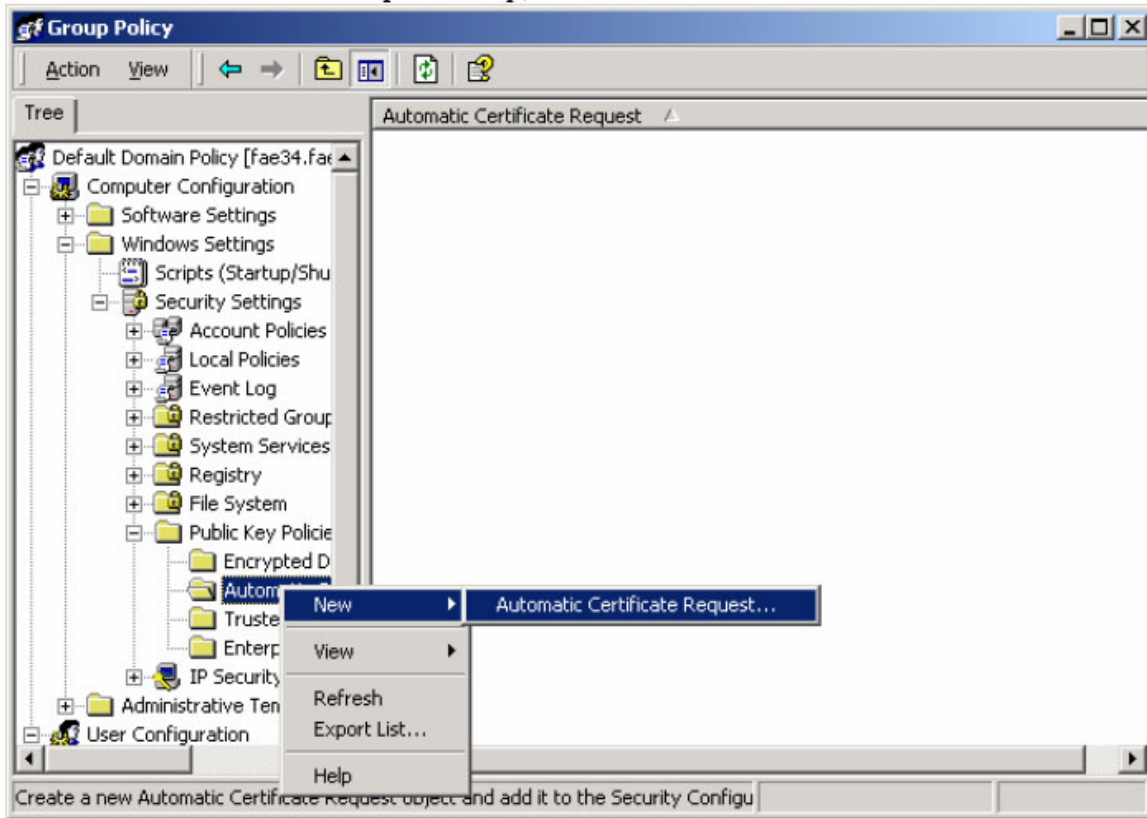
7. Select “Group Policy” tab and tick “default Domain Policy” click on “Properties”.



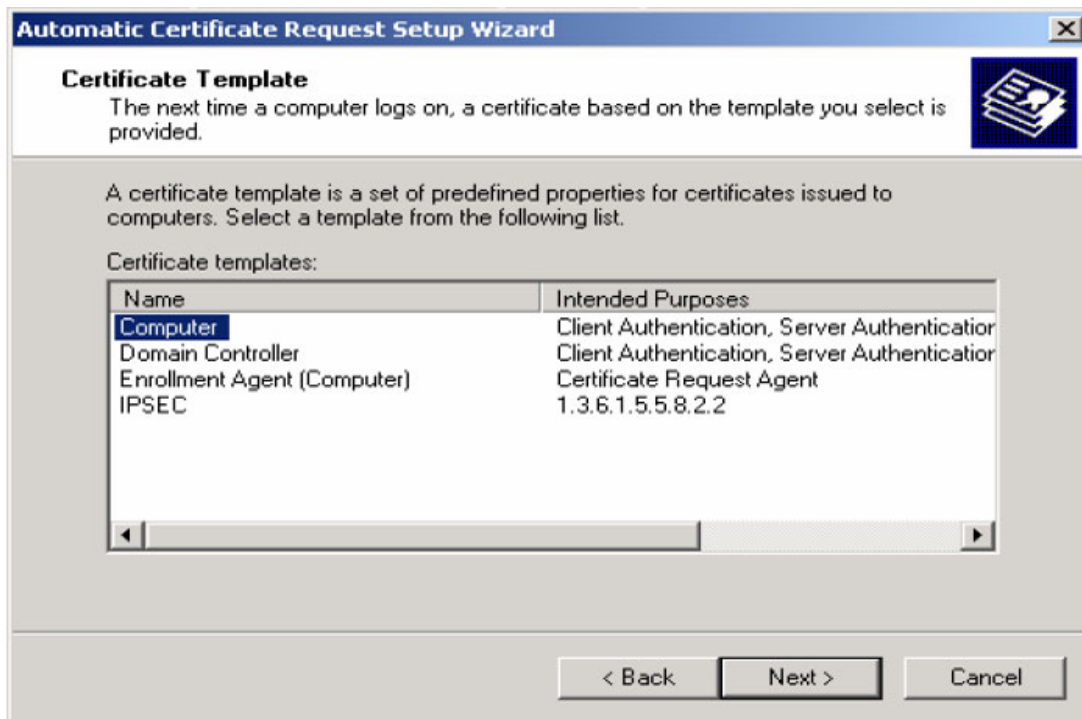
8. Select Computer configuration > Security Setting > Public Key Policies

9. Right Click “Automatic Certificate Request Setting”, select “New” then click on “Automatic Certificate Request”.

10. The Automatic Certificate Request Setup Wizard will guide you through the Automatic Certificate Request Setup, Click next to continue.



11. Select "Computer" certificate template and press "Next".



12. Press "Complete" to finish Automatic Certificate Request configuration Wizard.

13. Go to Start > Run type "CMD" press Enter.

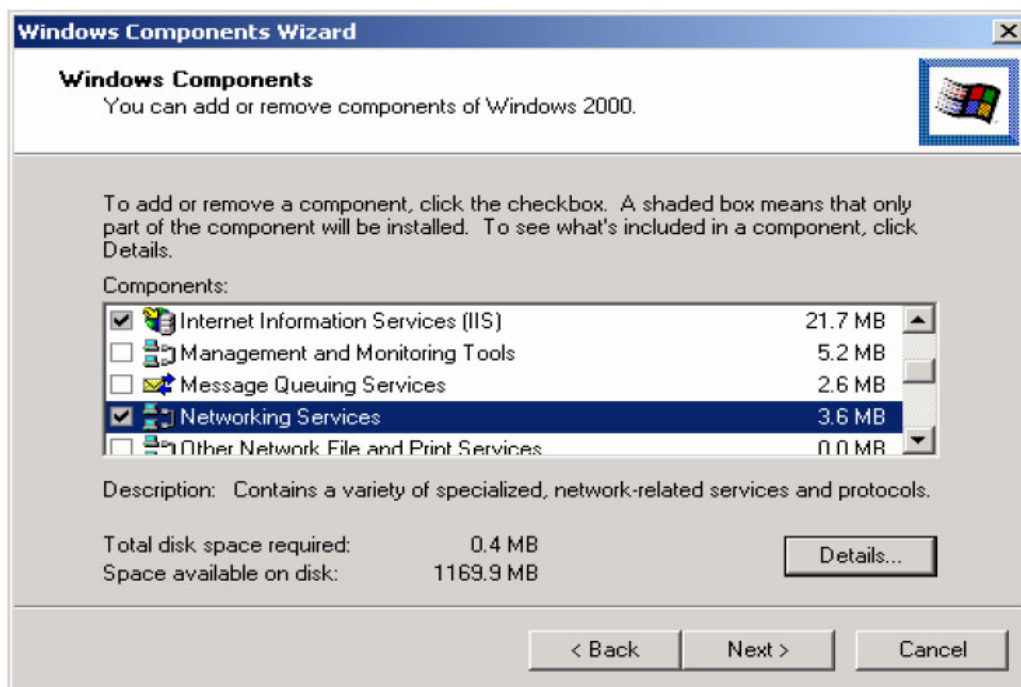
14. Under Dos command type "c:\secedit/refreshpolicy machine_policy" and press Enter.

```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

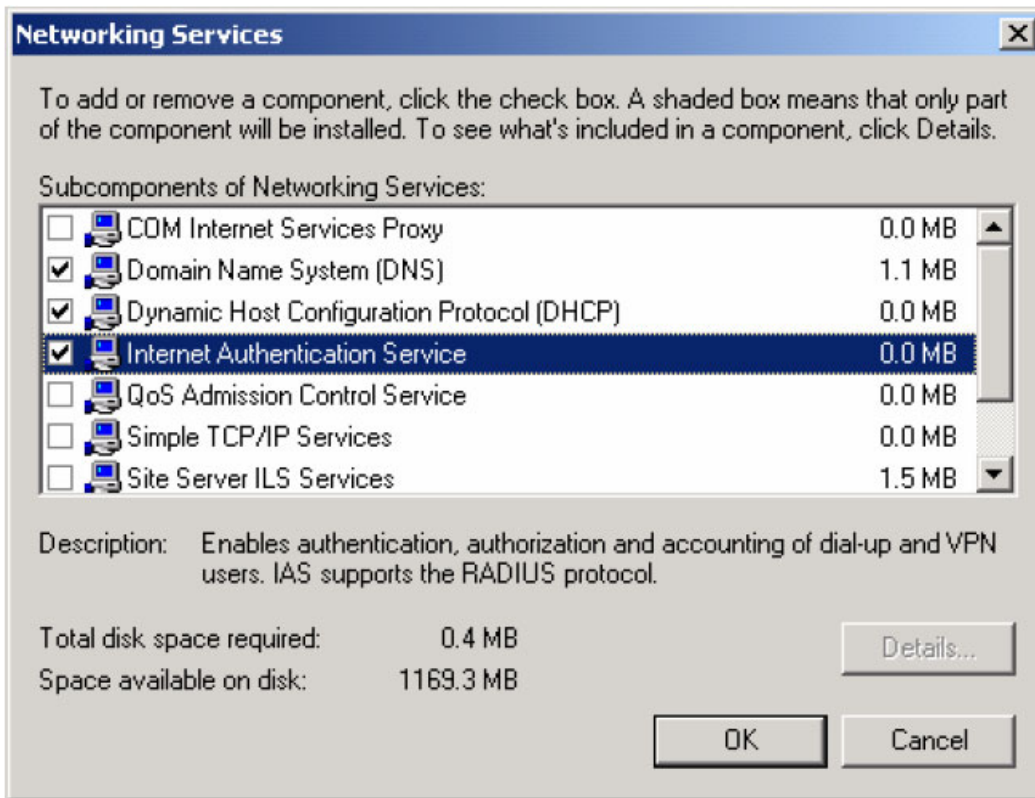
C:\>secedit/refreshpolicy machine_policy
Group policy propagation from the domain has been initiated for this computer. I
t may take a few minutes for the propagation to complete and the new policy to t
ake effect. Please check Application Log for errors, if any.
C:\>_
```

Step3: Internet Authentication Service (Radius) Configuration

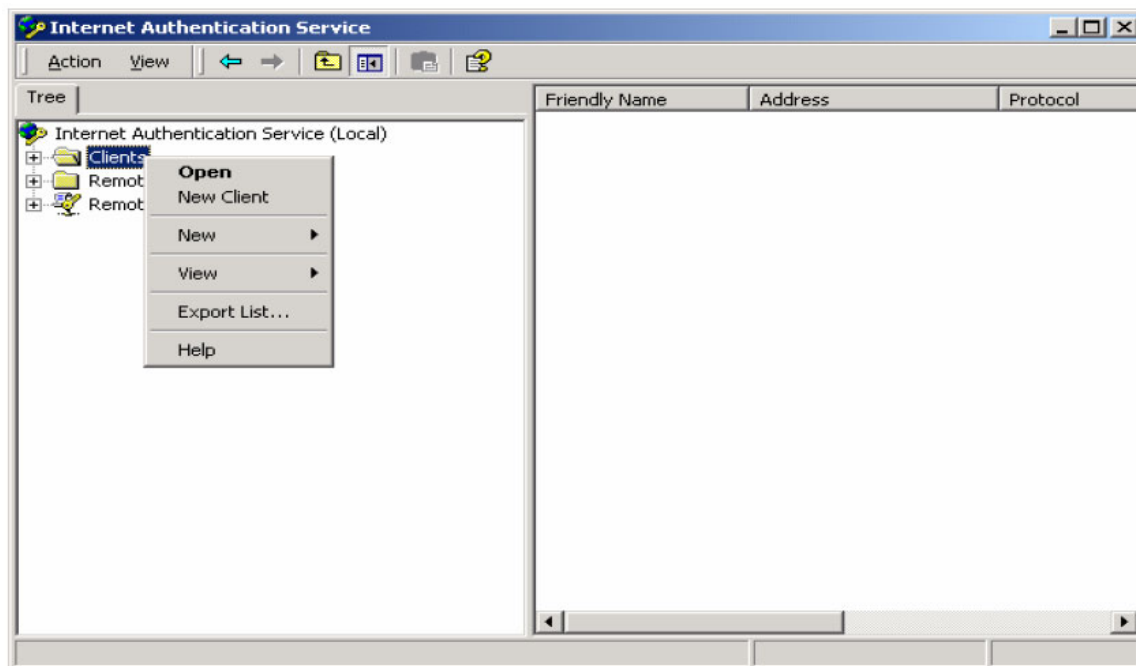
1. Go to Start > Control Panel > Add or remove programs
2. Select "Add or Remove Windows Components", select "Network Services"



3. Press "Details..." and select "Internet Authentication Service"



4. Go to Start > Programs > System Administrative Tools > Internet Authentication Service.
5. Right Click on "Client" and select "New Client".



6. Put a name to represent your Access Point and press "Next".
7. Key in a share key for this Access Point.
8. Press "Finish" to complete.

Add RADIUS Client

Client Information
Specify information regarding the client.

Client address (IP or DNS):

Client-Vendor:

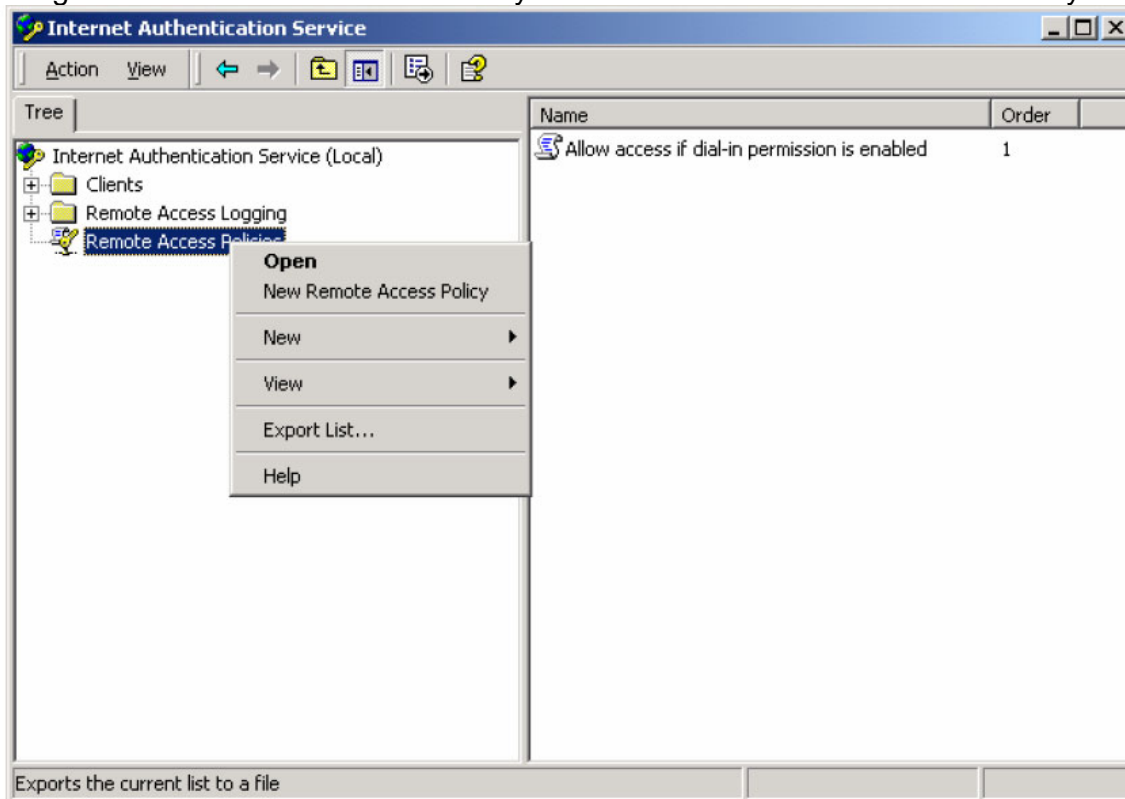
Client must always send the signature attribute in the request

Shared secret:

Confirm shared secret:

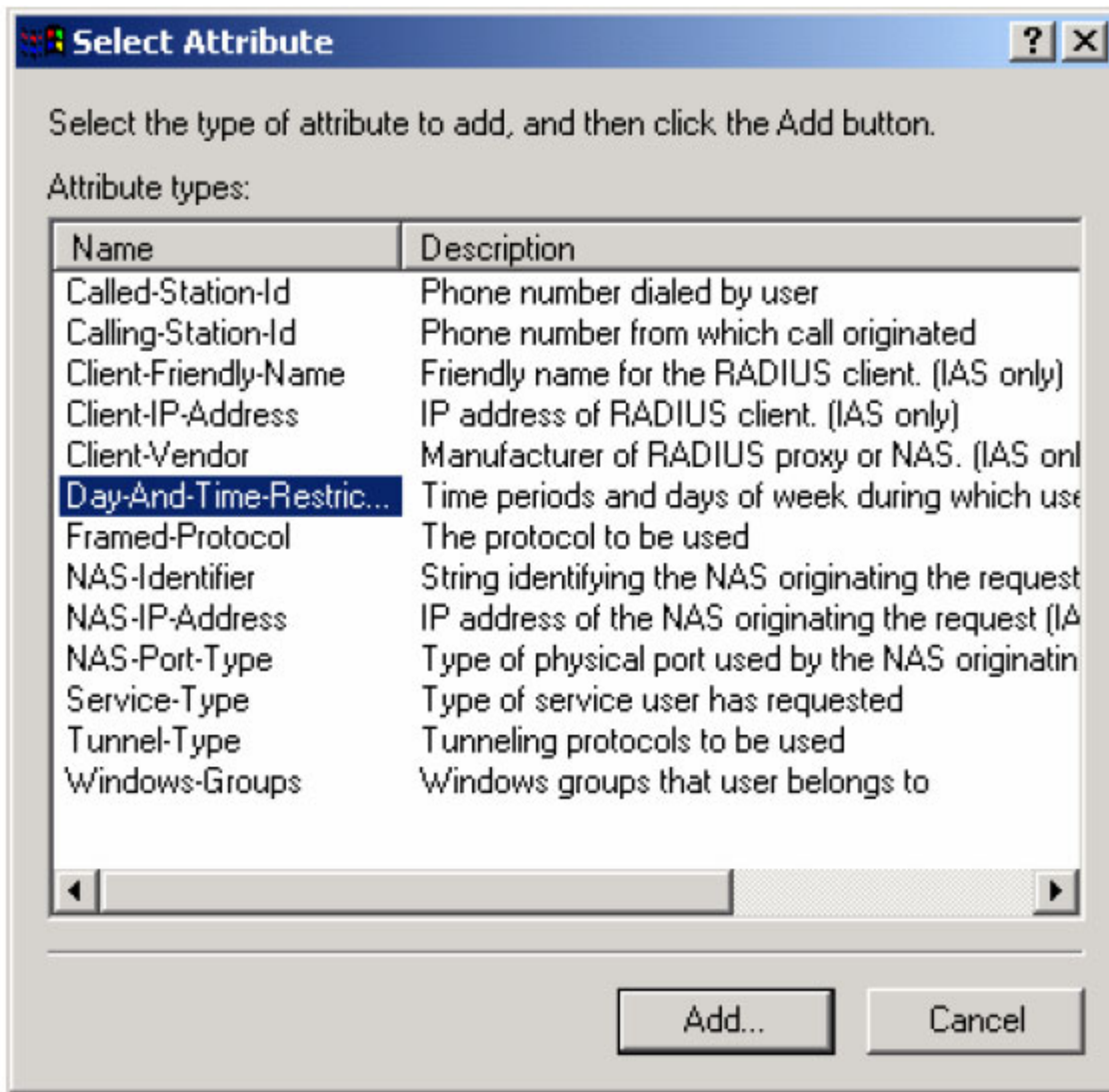
< Back

9. Right click on “Remote Access Policy” and select “New Remote Access Policy”

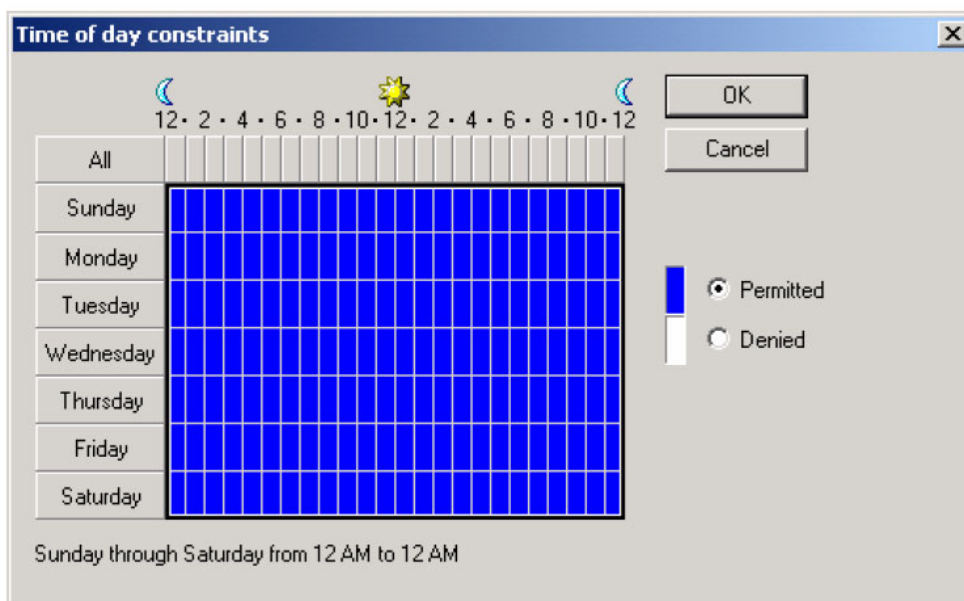


10. Type a name for new policy, press “Next”.

11. Select “Day-And-Time-Restrictions” press “Add”.

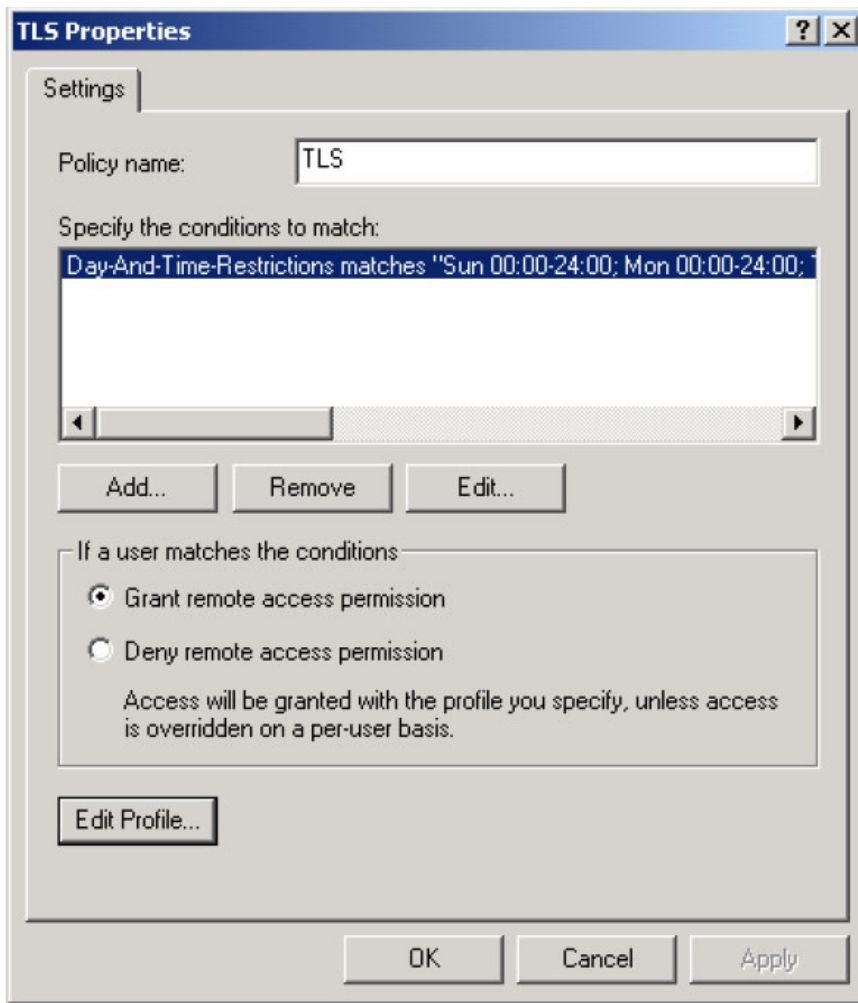


12. Tick "Permitted" and select this service operation time.

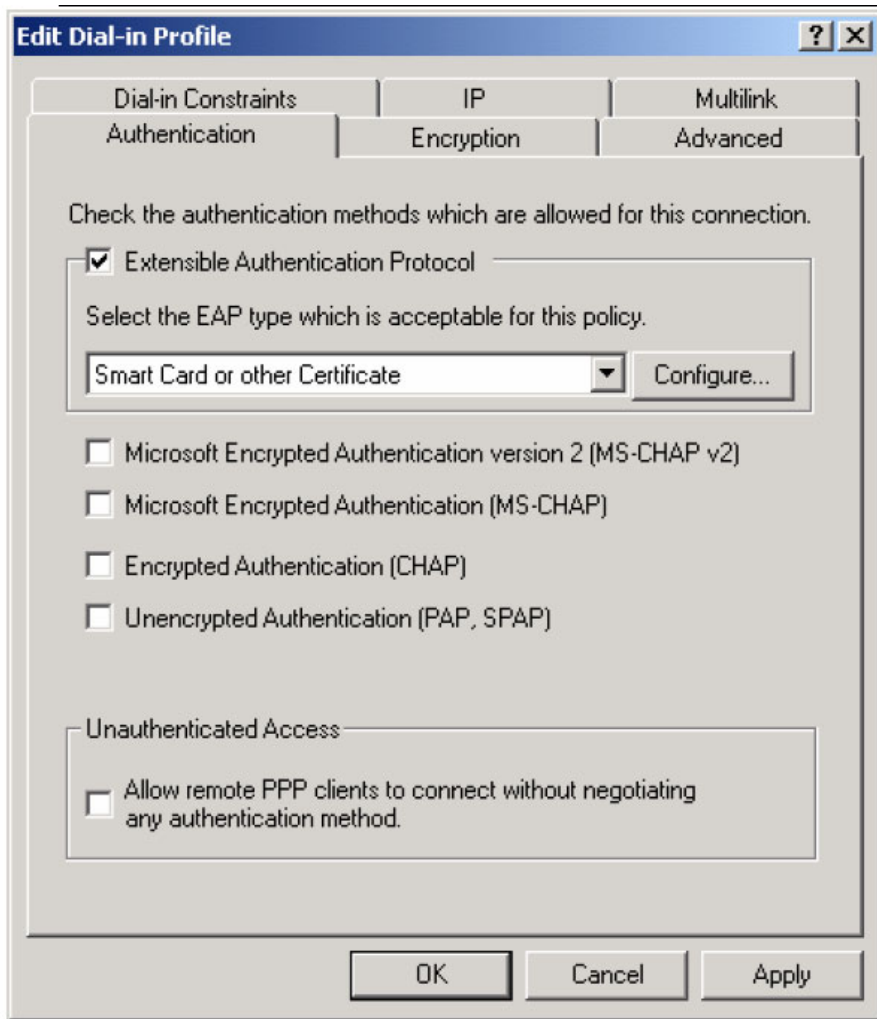


13. Tick "Grant remote access permission" and click "Next".

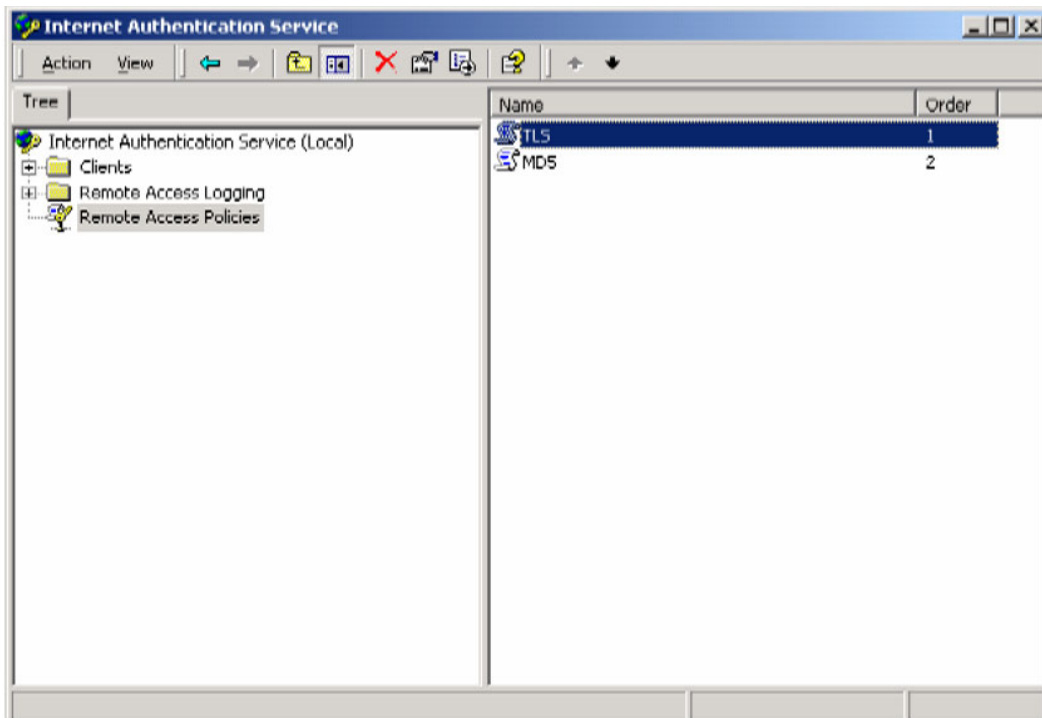
14. Press "Edit Profile"



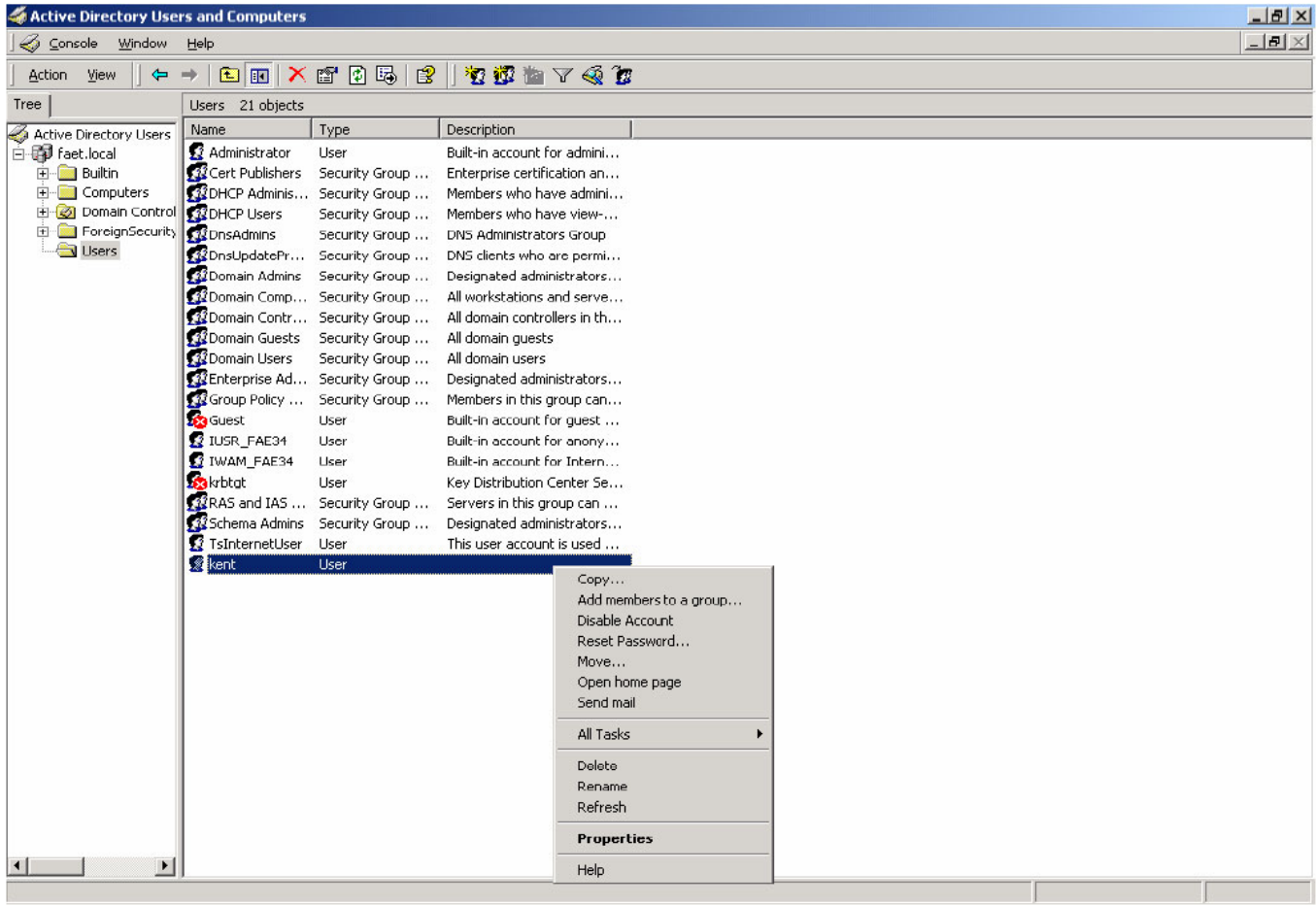
15. Select Authentication method: tick "Extensible Authentication Protocol" and select "Smart Card or other Certification" under Authentication. Press "OK" to complete configuration.
Note: If you need other authentication methods please select them here.



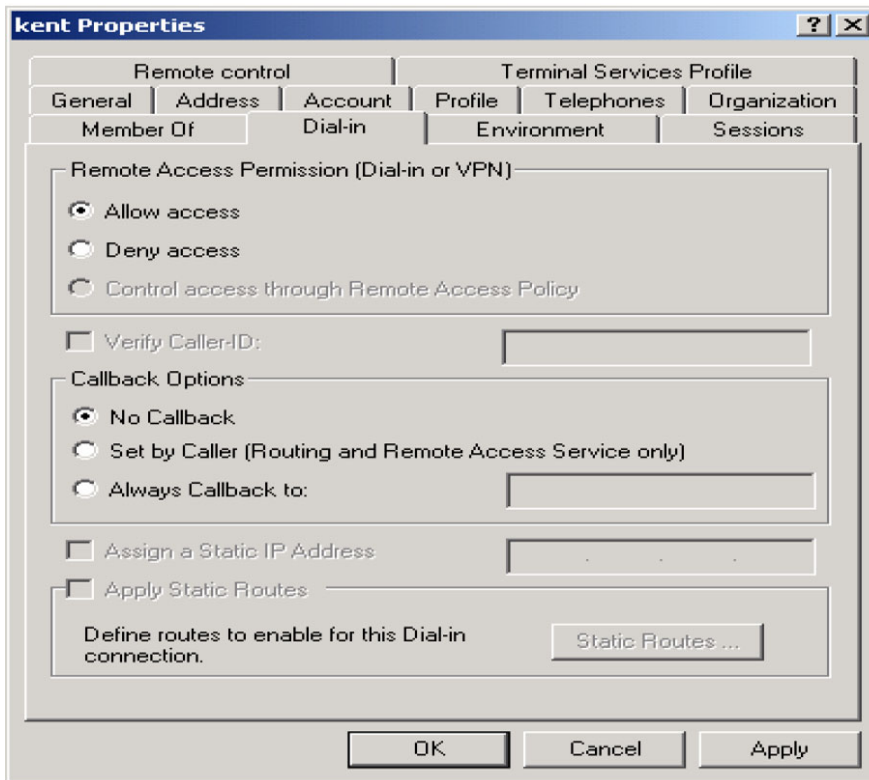
16. Put this policy to be first (please confirm the policy order).



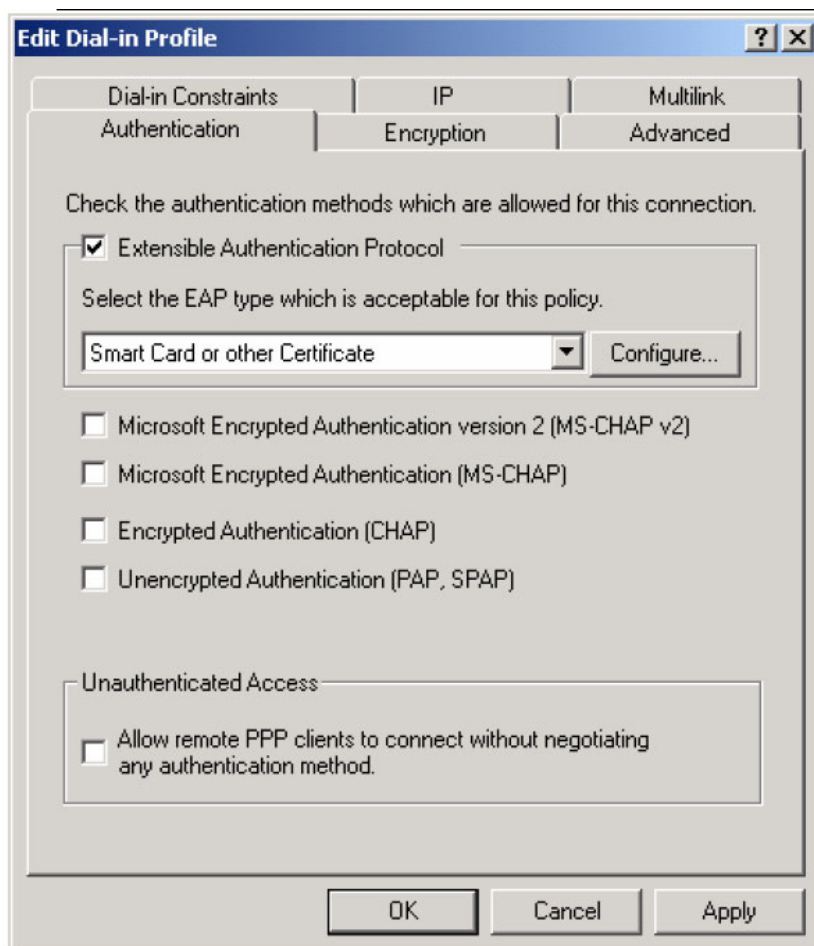
- 17. Go to Start > Programs > System Administrative tools > Active Directory Users and Computers
- 18. Right click on the user who needs this service.



- 19. Select "Dial-in", tick "Allow Access" in Remote Access Permissions and press "OK" to complete the configuration.



Note: If you will be using another authentication method (example: MD5 needs CHAP), please go to "Authentication" page. TLS can use the default values.



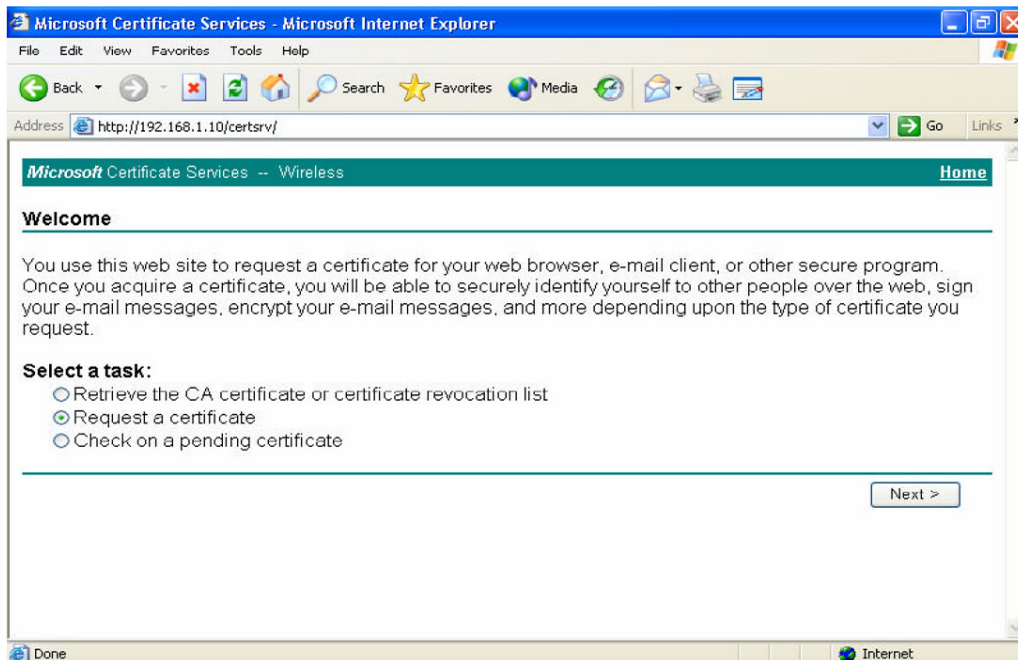
Part 3-2: 802.1x TLS Logon

Step 1: Get a CA

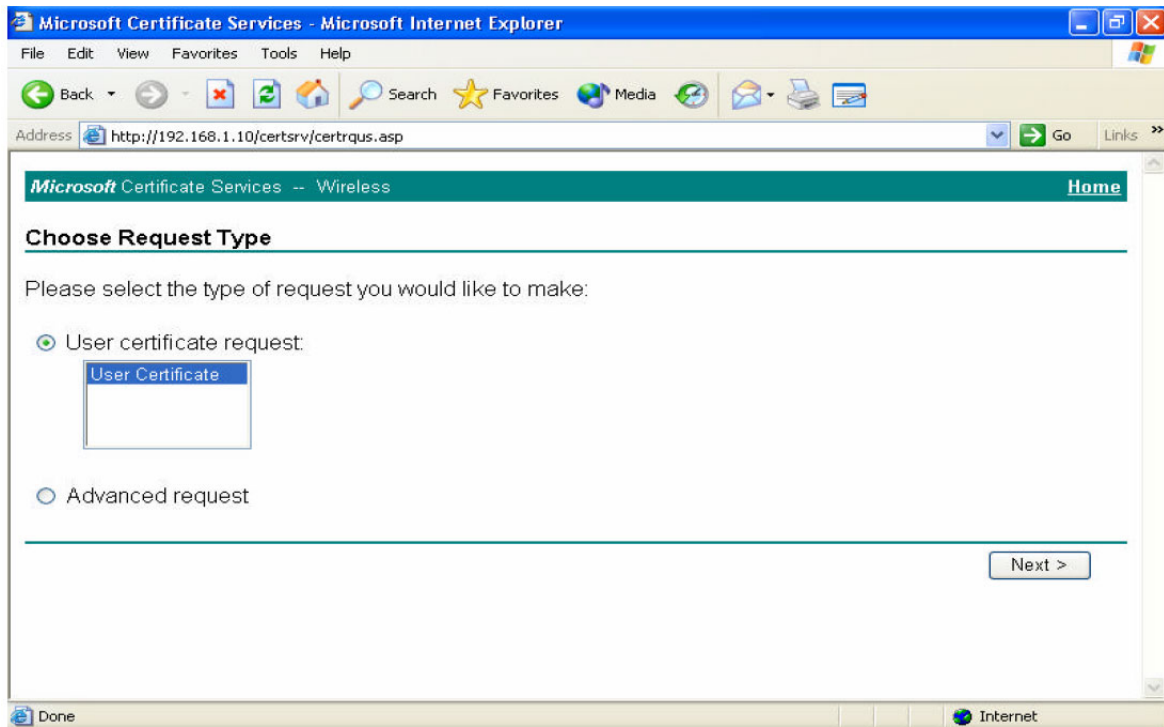
1. Connect your computer to the network with RADIUS Server (use wired connection. Otherwise disable all security settings on your wireless connection).
2. Open you WEB browser (for Example IE). In the address bar type "RADIUS Server IP/certsrv" (for example "192.168.1.10/certsrv"). Please make sure IIS service of your Windows 2000 server is turned on.
3. Server will return a message with username/password request. Please type your username/password (you setup this up in the previous step).



4. Microsoft Certificate Service --- Wireless page will come up. Select "Request a Certificate" and press "Next".



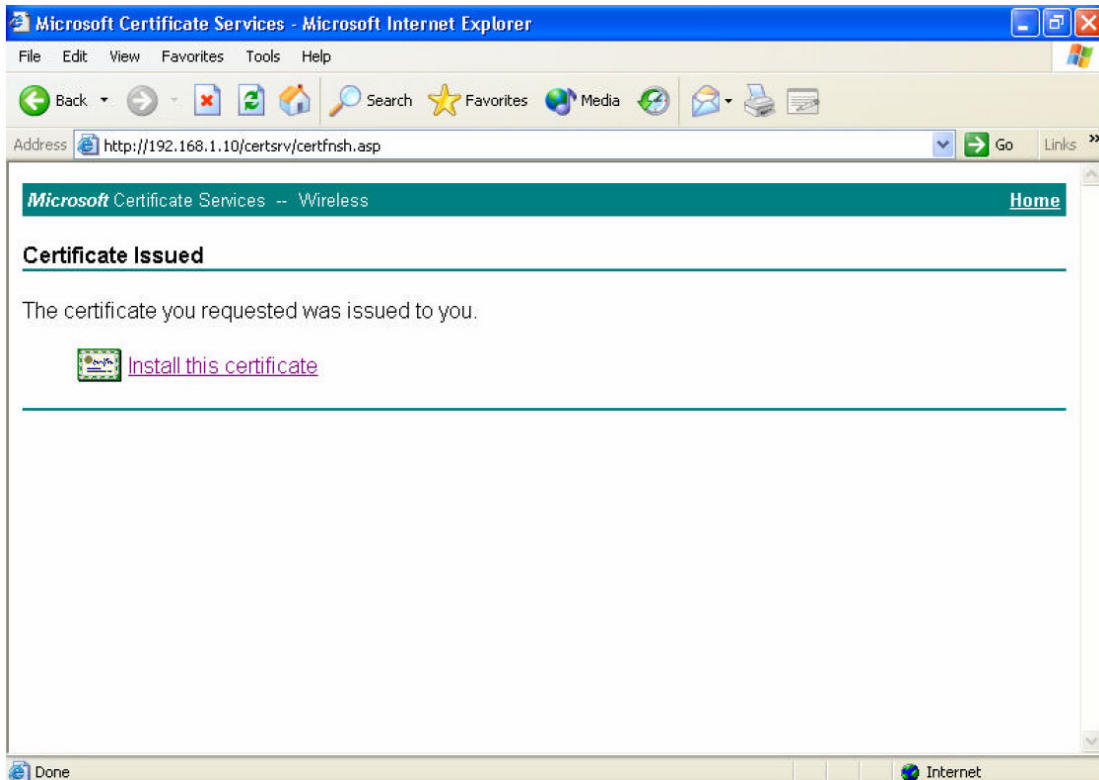
5. Select "User certificate request" press "Next".



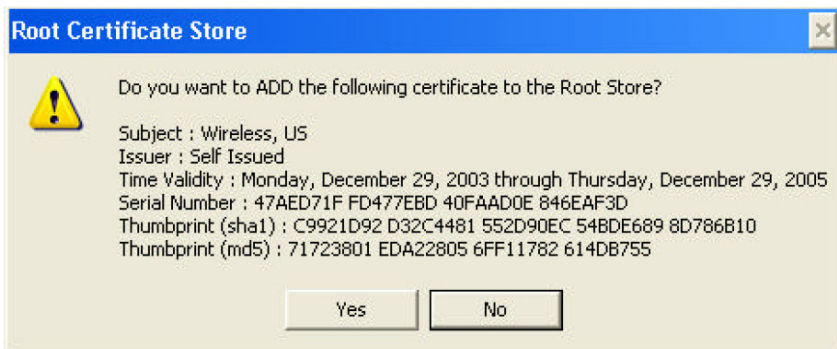
6. User Certificate – Identifying Information, press “Submit”.
7. CA warning message will pop up, press “Yes”.



8. Click “Install this certificate”



9. Confirm adding this CA, press “Yes”.



10. Certificate Installed.

Step 2: Access Point Configuration

1. Log into the Access Point using your WEB Browser. Open Access Point Security configuration page.

2. Select “802.1x”

- 3. Fill in the configuration fields on this page:
- Lifetime: How frequently the Key is changed
- Length: Encryption Length
- IP: RADIUS Server IP
- Port: Service Port (Standard RADIUS port 1812)
- Shared Secret : Share key on RADIUS server (the one you set up for this AP)

Note: If you have a Backup Server please setup RADIUS server 2 as well.

D-Link
Building Networks for People

AirPlus Xtreme G™
High-Speed 2.4GHz Wireless Access Point

DWL-2000AP

Mode
Performance
Filters
802.1X

Home Advanced Tools Status Help




802.1X

Enabled Disabled

Encryption Key Length 64 bits 128 bits
Lifetime 30 Minutes

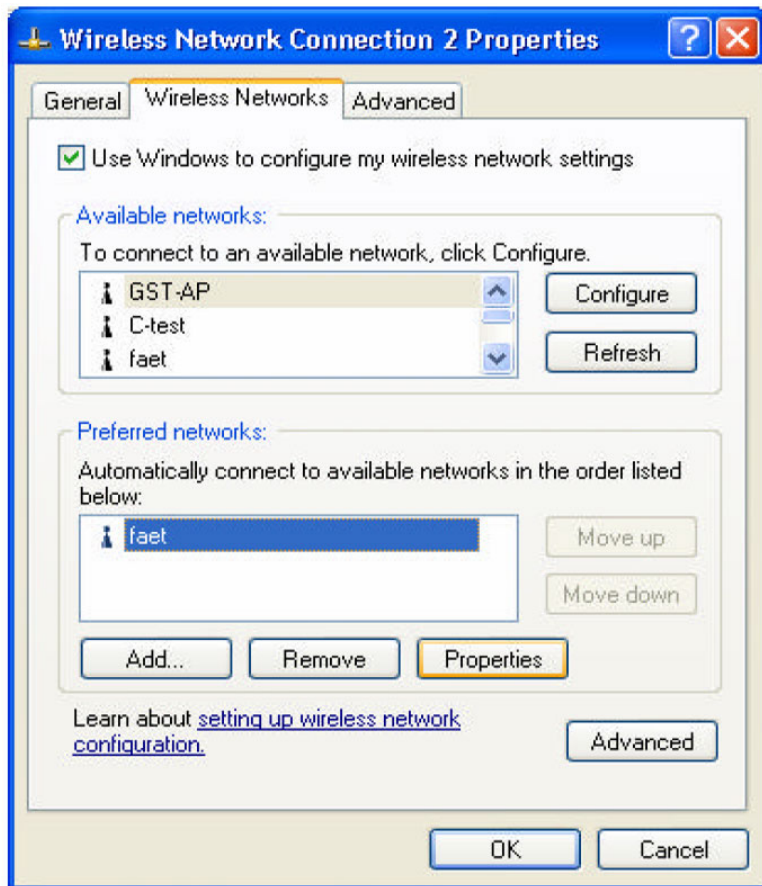
RADIUS Server 1
IP 192.168.0.10
Port 1812
Shared Secret

RADIUS Server 2 (Optional)
IP 0.0.0.0
Port 0
Shared Secret

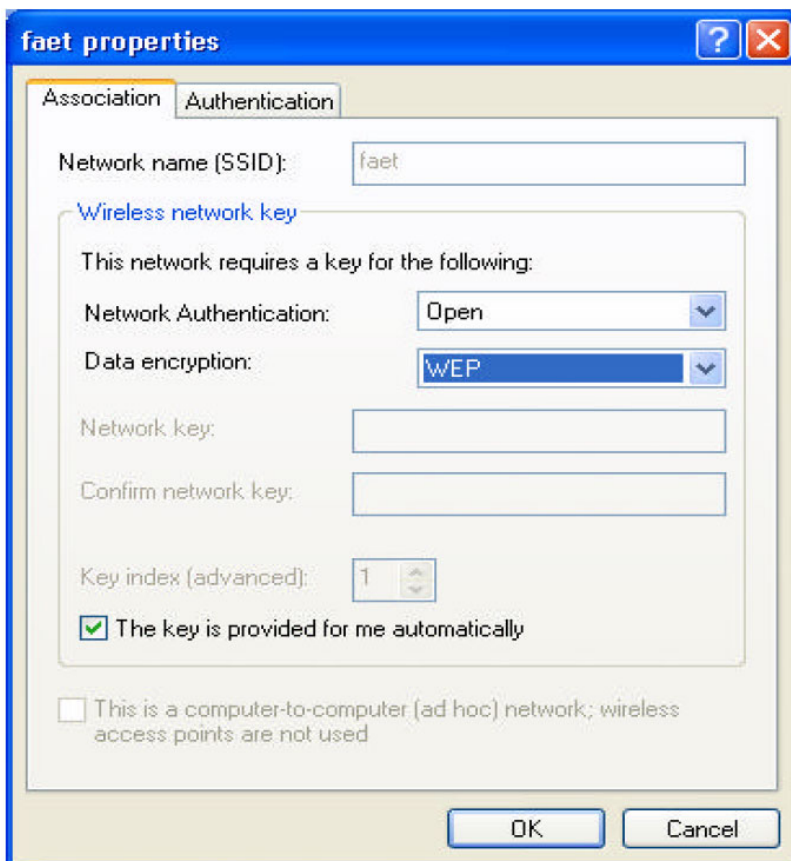
  
Apply Cancel Help

Step 3: 802.1x Connection

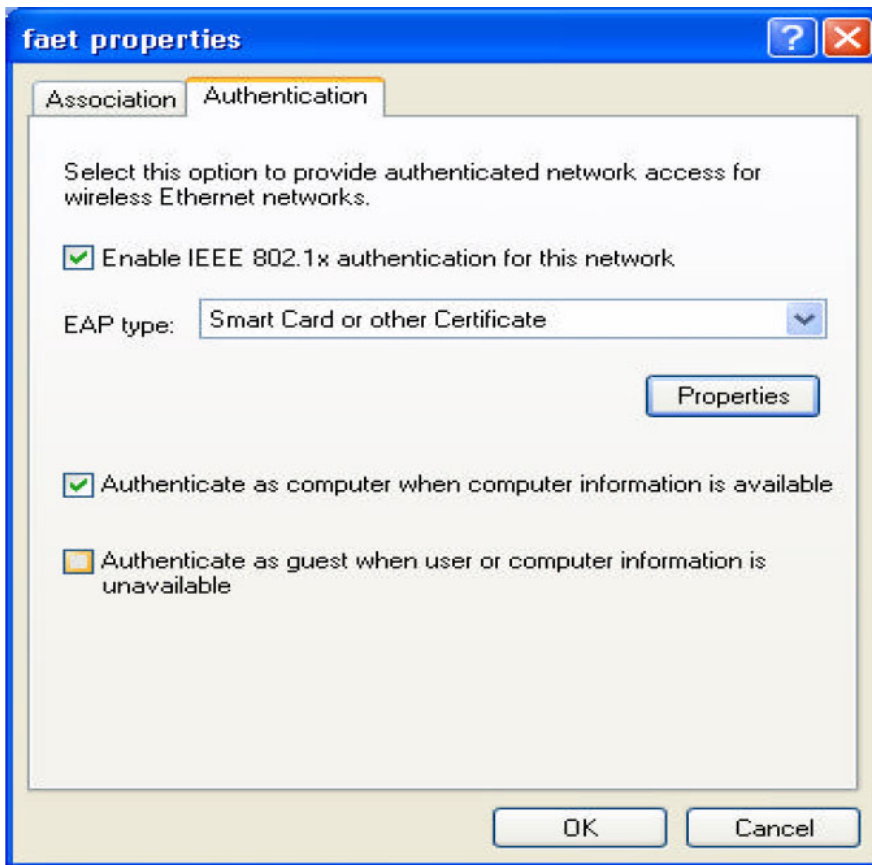
1. We will use Windows XP Wireless Utility as an example.
2. Right click on "My Network Places" on your desktop and select "Properties" (or go to Start > Control Panel > Network).
3. Select your Wireless LAN Card, right-click and select "Properties".
4. Click "Wireless Network".
5. Select the Access Point which you are going to connect to and click "Configure"



6. Select "OPEN System" under Network Authentication. Select WEP encryption. Tick "The key is provided for me automatically".



7. Select "Authentication" page. Tick "Enabled IEEE 802.1xAuthentication for this Network", Under EAP Type select "Smart Card or other certificate". Press "OK".



8. When your workstation will be connecting to the AP you will see the Authentication process window. Click on it and you will see a pop up window as below. (If there is more than one CA on your system you will see a CA selection screen first).



Note: Newer versions of Windows can handle it automatically; you may not see the last step.

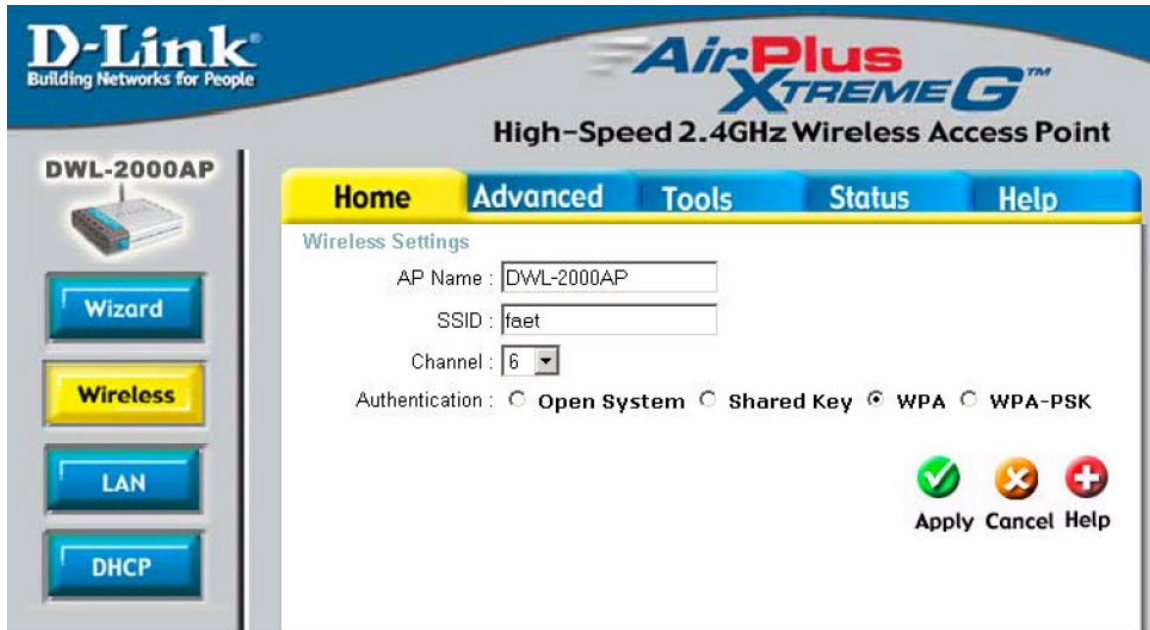
Part 3-3: WPA Logon

Step 1: Request CA

Please see to the steps for setting up 802.1x to request CA

Step 2: AP Configuration

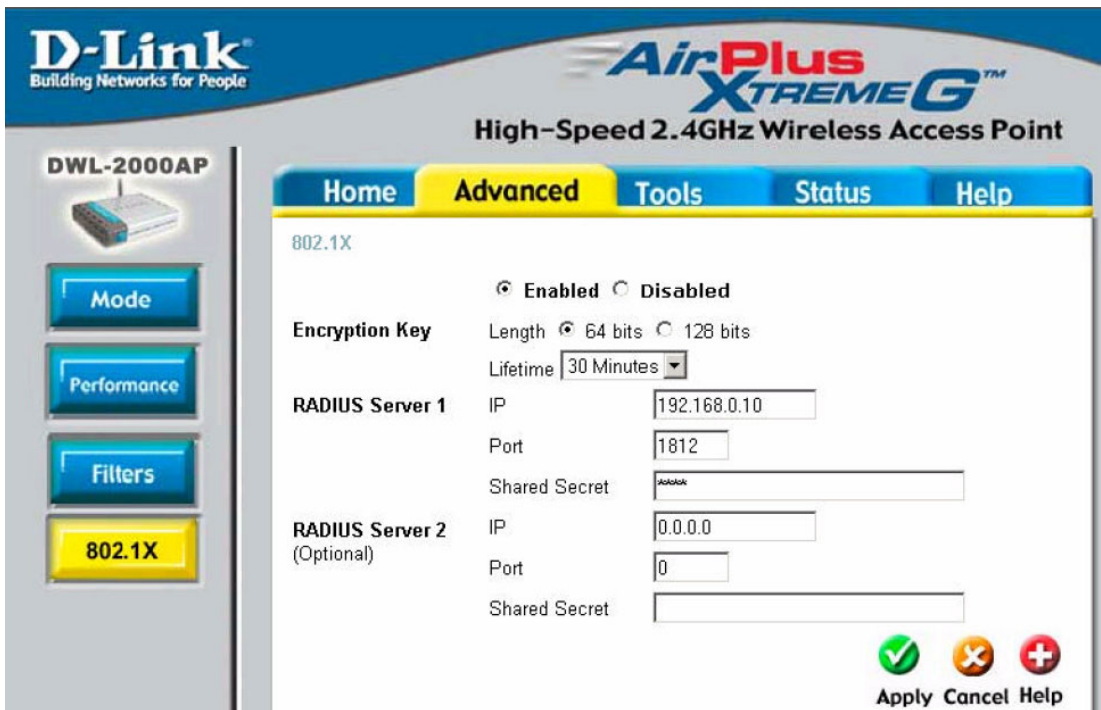
1. Log into your Access Point using your WEB Browser (e.g. Internet Explorer). Open security web page on your Access Point.
2. Select WPA on this page, press "Apply".



3. Go 802.1x Configuration page

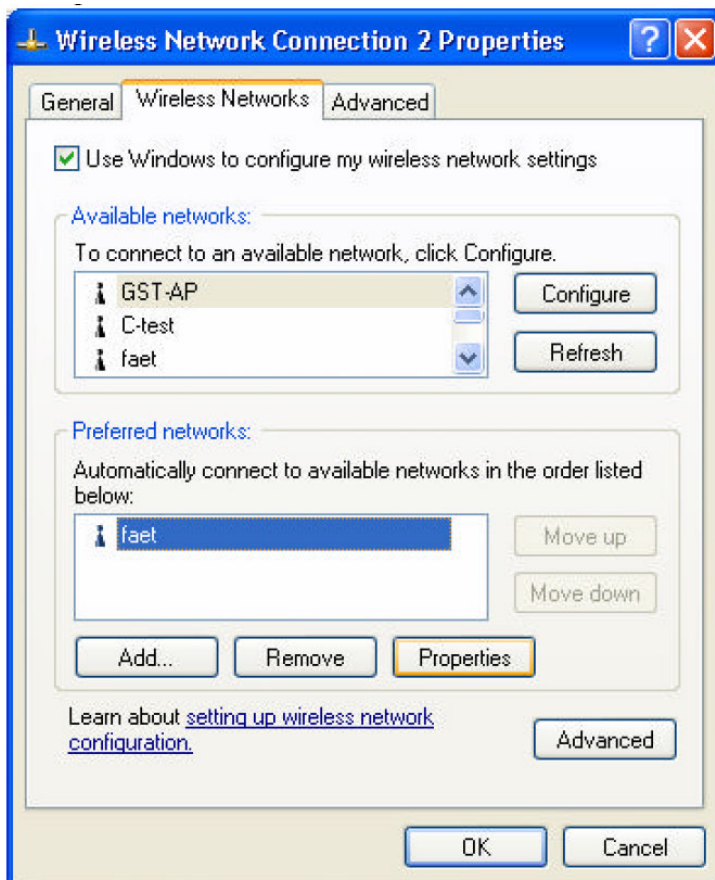
- 3. Fill in the configuration fields on this page:
- Lifetime: How frequently the Key is changed
- Length: Encryption Length
- IP: RADIUS Server IP
- Port: Service Port (Standard RADIUS port 1812)
- Shared Secret : Share key on RADIUS server (the one you set up for this AP)

Note: If you have a Backup Server please setup RADIUS server 2 as well.

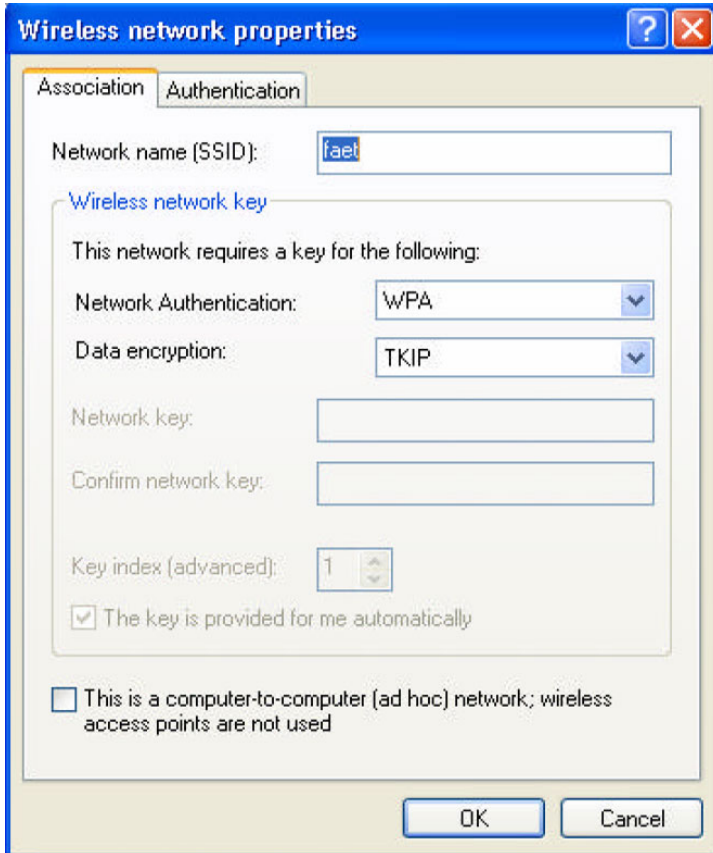


Step 3: Connection as WPA

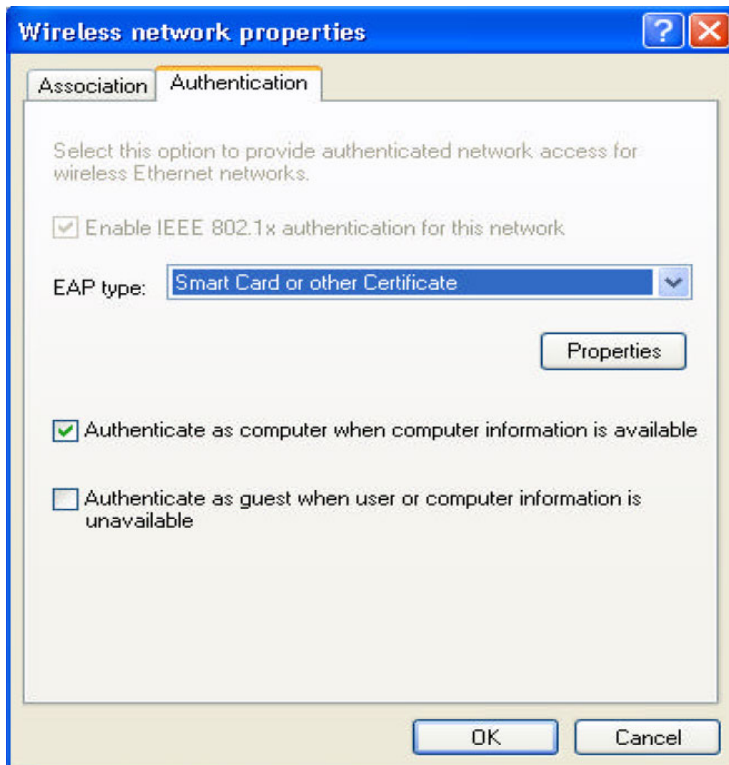
1. We will use Windows XP Wireless Utility as an example.
2. Right click on "My Network Places" on your desktop and select "Properties" (or go to Start > Control Panel > Network).
3. Select your Wireless LAN Card, right-click and select "Properties".
4. Click "Wireless Network".
5. Select the Access Point which you are going to connect to and click "Configure"



6. Select “WPA” under Network Connection, and use “TKIP” for Data Encryption.



7. Select EAP type "Smart Card or other Certificate", Press "OK" to complete the setup.



8. When your workstation will be connecting to the AP you will see the Authentication process window. Click on it and you will see a pop up window as below. (If there is more than one CA on your system you will see a CA selection screen first).

Note: Newer versions of Windows can handle it automatically; you may not see the last step.



~ End of Document ~