Wireless Network Security

Part 1: WEP

Step1: Configuration Access Point's WEP key.

1. Go WEP configuration page where you can find from your Access Point user manual. Tick WEP option which on the web page "Enabled".
2. Select "Key Mode".

   Normally two of Key mode you can select: ASCII or Hex

   ASCII (American Standard Code for Information Interchange):

   A standard for assigning numerical values to the set of letters in the Roman alphabet and typographic characters

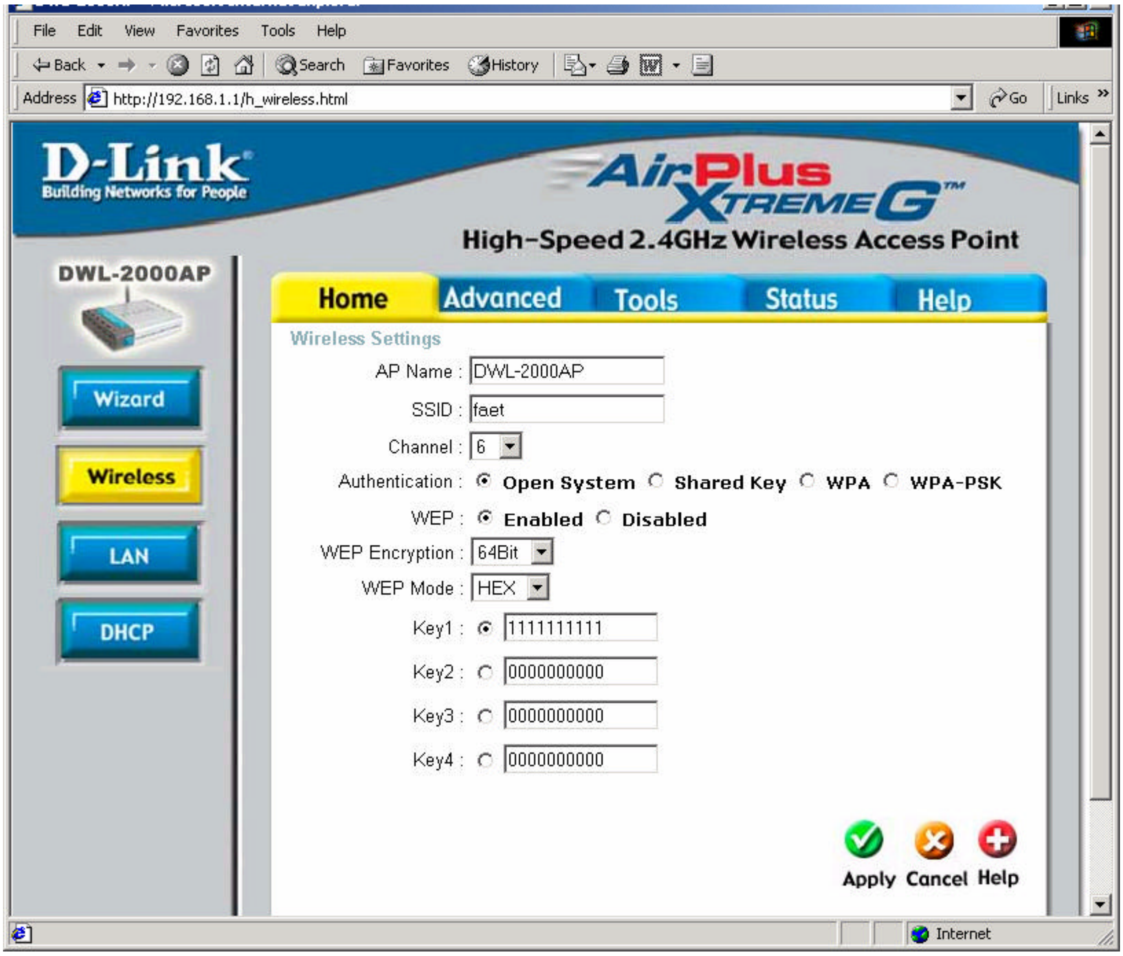
   HEX (Hexadecimal):

   The ordinal number from 0 to 9, a to f.
3. Select WEP Key length.

   64 bit: 5 of ASCII or 10 of Hex

   128 bit: 13 of ASCII or 26 of Hex
4. Select default key.

   In standard, there are 4 groups of WEP key can be used. Default key is the one Access Point check when a station connected (for stations default key is to check when connected to an Access Point). WEP key can be ignore if Access Point and Station do not use them (for example if both AP and station select key 1 another three keys are no need to set)


File Edit View Favorites Tools Help
Back
Search
Favorites
History
Address http://192.168.1.1/h_wireless.html
Go
Links
D-Link
Building Networks for People
AirPlus
XTREME G
High-Speed 2.4GHz Wireless Access Point
DWL-2000AP
Home
Advanced
Tools
Status
Help
Wizard
Wireless
LAN
DHCP
Apply
Cancel
Help
Internet

Wireless Settings

AP Name : DWL-2000AP

SSID : faet

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

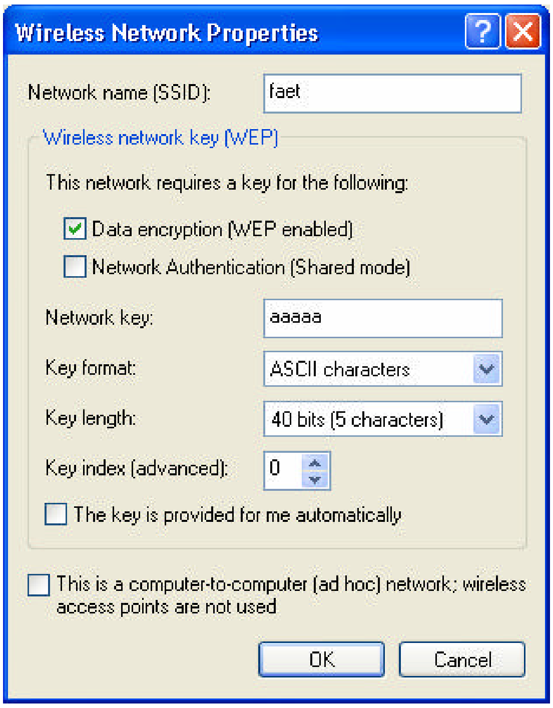
Key4 : ○ 0000000000

5. Press “Apply” to complete your settings.

Step 2: Configuration Station’s WEP Key.

1. Here will only use Windows XP as a sample for Station’s WEP key setting.
2. Right click “My Network Place” on your desktop and click “Properties” (or go to “Start/ Settings/ Network” or double click a network icon which represents your wireless network on system tray where right down your screen).
3. Select your Wireless LAN Card right clicks and selects “Properties”.
   Click “Wireless Network”.
4. Select the Access Point which you going to connect and click “Configuration” on its right.
5. See “Wireless Network Properties” and tick up “Data encryption (WEP Enabled)”.
   Tick off “The key is provided for me automatically”.

6. Select "key index" which is the default key for your station (Note: Some Windows versions the indexes are from 0 to 3 it map to 1 to 4 as usual).
7. Key in your WEP Key value into "Network Key".
8. Press "OK" to finish your station setting.



Wireless Network Properties

Network name (SSID): faet

Wireless network key (WEP)

This network requires a key for the following:

☑ Data encryption (WEP enabled)

□ Network Authentication (Shared mode)

Network key: aaaaa

Key format: ASCII characters

Key length: 40 bits (5 characters)

Key index (advanced): 0

□ The key is provided for me automatically

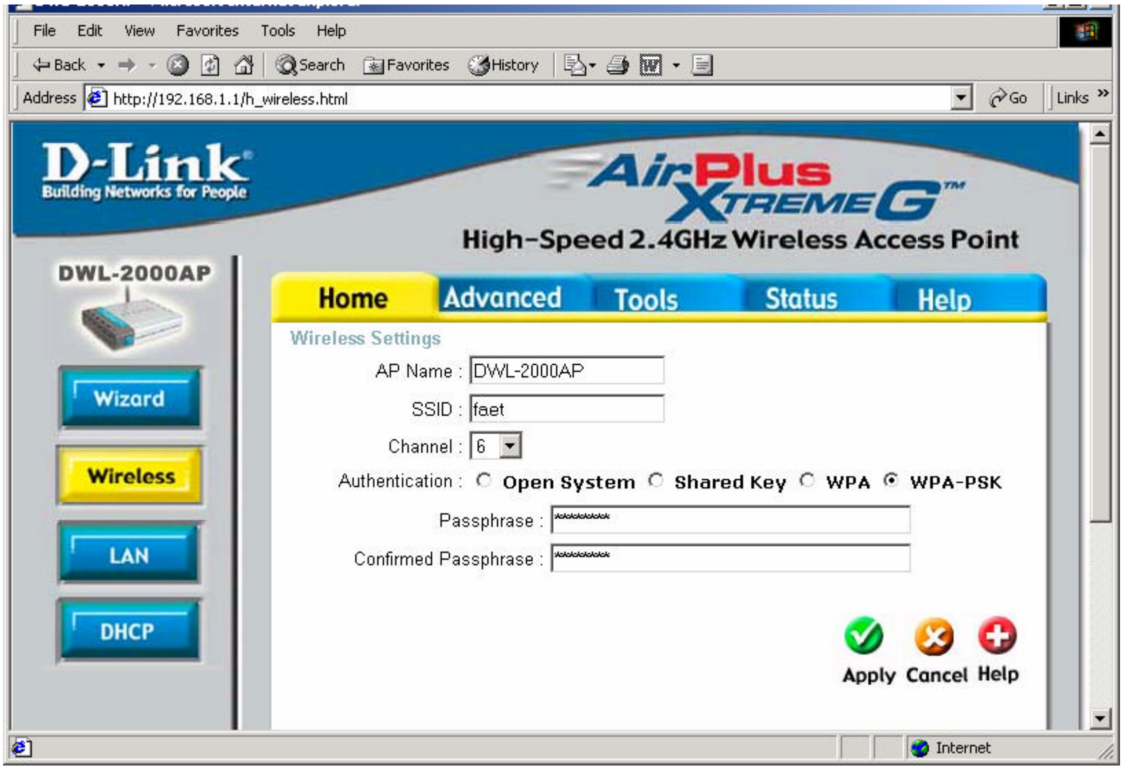
□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Part 2: WPA-PSK

Cause of WPA-PSK is extending of WEP key, so its configuration will very close to WEK key which is mach key between Access Point and Stations.

Step1: Configuration Access Point's WPA-PSK

1. Go WPA-PSK configuration page where you can find from your Access Point user manual.
2. Key in your security code (unless eight characters)
3. Press "Apply" to complete Access Point's configuration.



Address http://192.168.1.1/h_wireless.html

Wireless Settings

AP Name : DWL-2000AP

SSID : faet

Channel : 6

Authentication : ○ Open System ○ Shared Key ○ WPA ● WPA-PSK

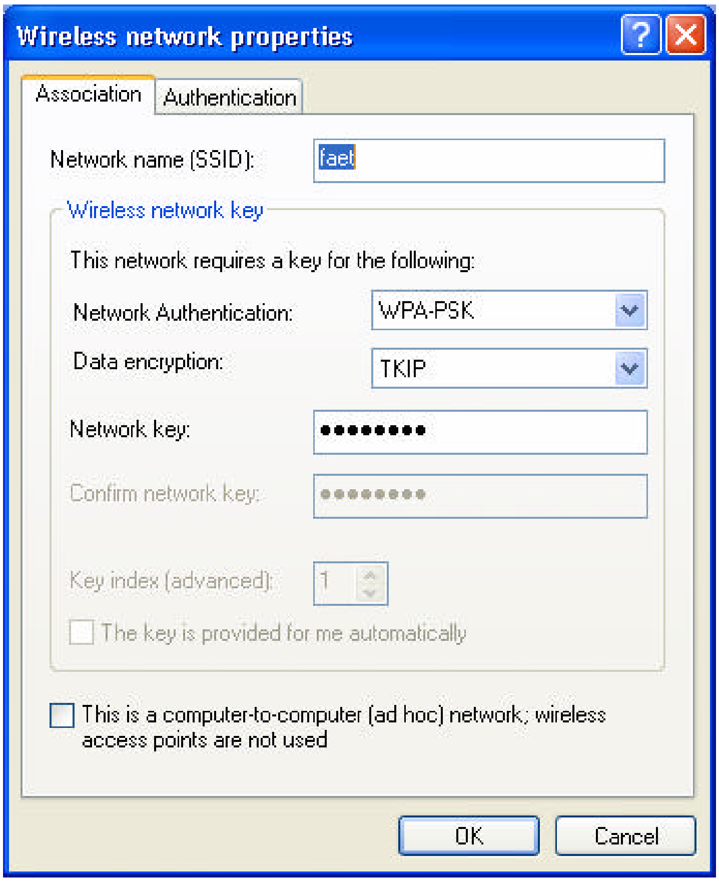
Passphrase : ********

Confirmed Passphrase : ********

Step2: Configuration Station's WPA-PSK

1. Here will use Windows XP sample for Station's WEP key setting.
2. Right click "My Network Place" on your desktop and click "Properties" (or go to "Start/ Settings/ Network" or double click a network icon which represents your wireless network on system tray where right down your screen).
3. Select your Wireless LAN Card right clicks and selects "Properties".

4. Click “Wireless Network”.
5. Select the Access Point which you going to connect and click “Configuration” on its right.
6. See “Wireless Network Properties/Association” and select “WPA-PSK” in “Network Authentication” then select “TKIP” in “Data encryption”. (AES standard is not finalized yes and most of product are not support AES on market).
7. Key in your “Network Key” which same as your Access Point and confirm it.
8. Press “OK” to finish your station setting.



Wireless network properties

Association | Authentication

Network name (SSID): faet

Wireless network key

This network requires a key for the following:

Network Authentication: WPA-PSK

Data encryption: TKIP

Network key: ●●●●●●●●●

Confirm network key: ●●●●●●●●●

Key index (advanced): 1

□ The key is provided for me automatically

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

Part 3: 802.1x and WPA

Part 3-1: RADIUS Server Installation

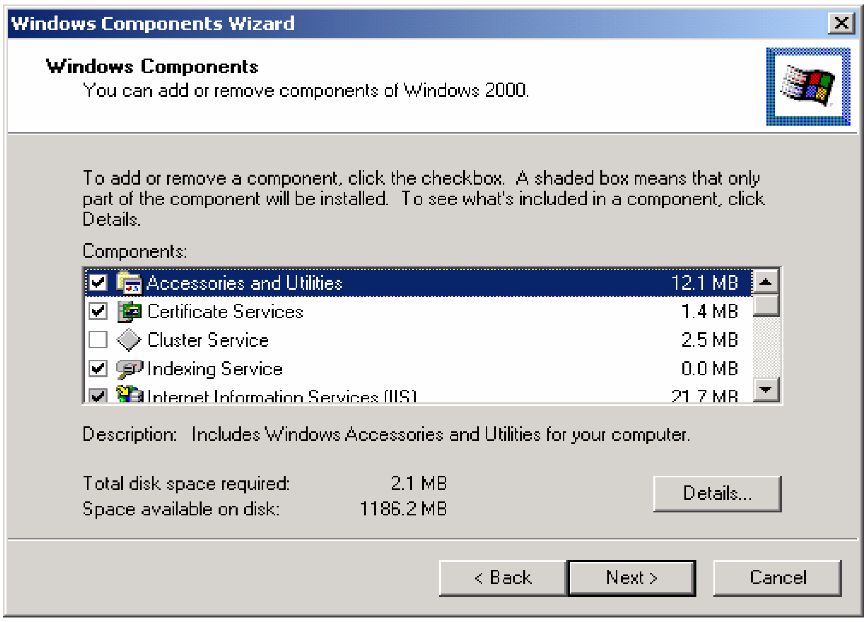
Firstly, we will configuration a RADIUS Server by using Windows 2000 Server and use 802.1x-TLS as sample.

<u>Prepare to set RADIUS Server up:</u>

- ❑ Windows 2000 Server has complete Active Directory configuration.
- ❑ The sample Server had been set be a Domain controller and DHCP/DNS is enabled on this server.
- ❑ For 802.1x, Windows 2000 Ser :ver upgrade to unless Service Pack 3 is needed.
- ❑ For WPA, Windows 2000 Server upgrade to unless Service Pack 4 is needed.

Step 1: Installation Certificate Authority

1. Logon into your Windows 2000 server as "Administrator or an ID has Administrator authority.
2. Go to "Start>control Panel>Add or Remove programs".
3. Select "Add or remove Windows Components".
4. Tick on "Certificate Service"and press "Next".



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.

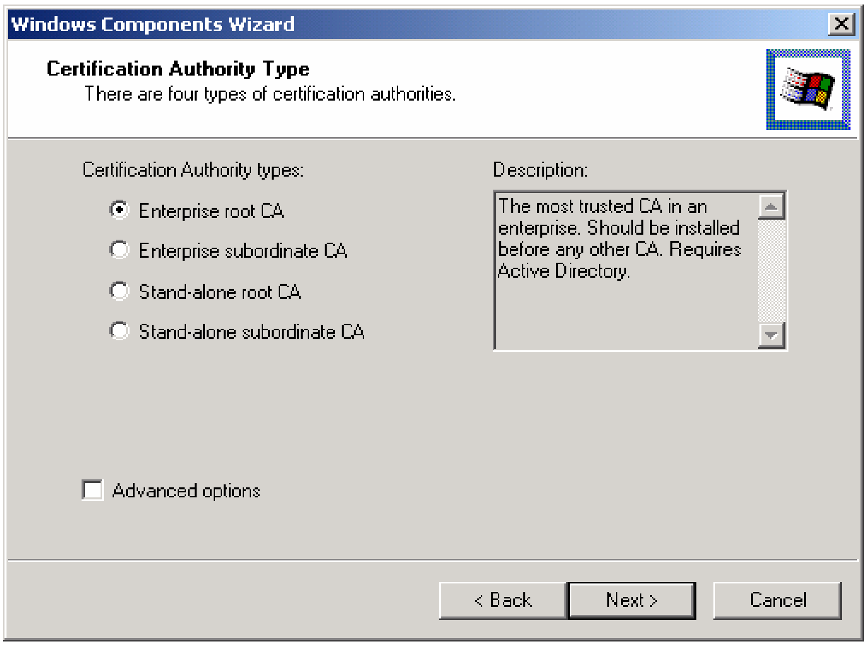
Components:

☑	Accessories and Utilities	12.1 MB
☑	Certificate Services	1.4 MB
□	Cluster Service	2.5 MB
☑	Indexing Service	0.0 MB
☑	Internet Information Services (IIS)	21.7 MB

Description: Includes Windows Accessories and Utilities for your computer.

Total disk space required: 2.1 MB
Space available on disk: 1186.2 MB

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



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

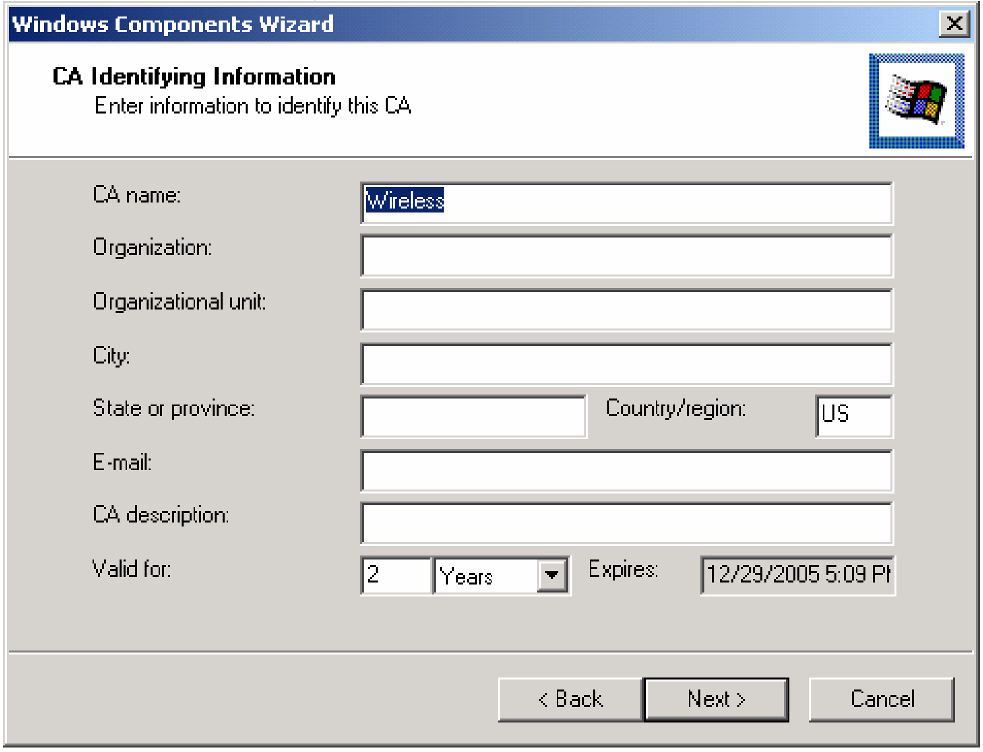
Description:

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

□ Advanced options

< Back | Next > | Cancel

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



Windows Components Wizard

CA Identifying Information

Enter information to identify this CA

CA name:	Wireless
Organization:	
Organizational unit:	
City:	
State or province:	
Country/region:	US
E-mail:	
CA description:	
Valid for:	2 Years
Expires:	12/29/2005 5:09 PI

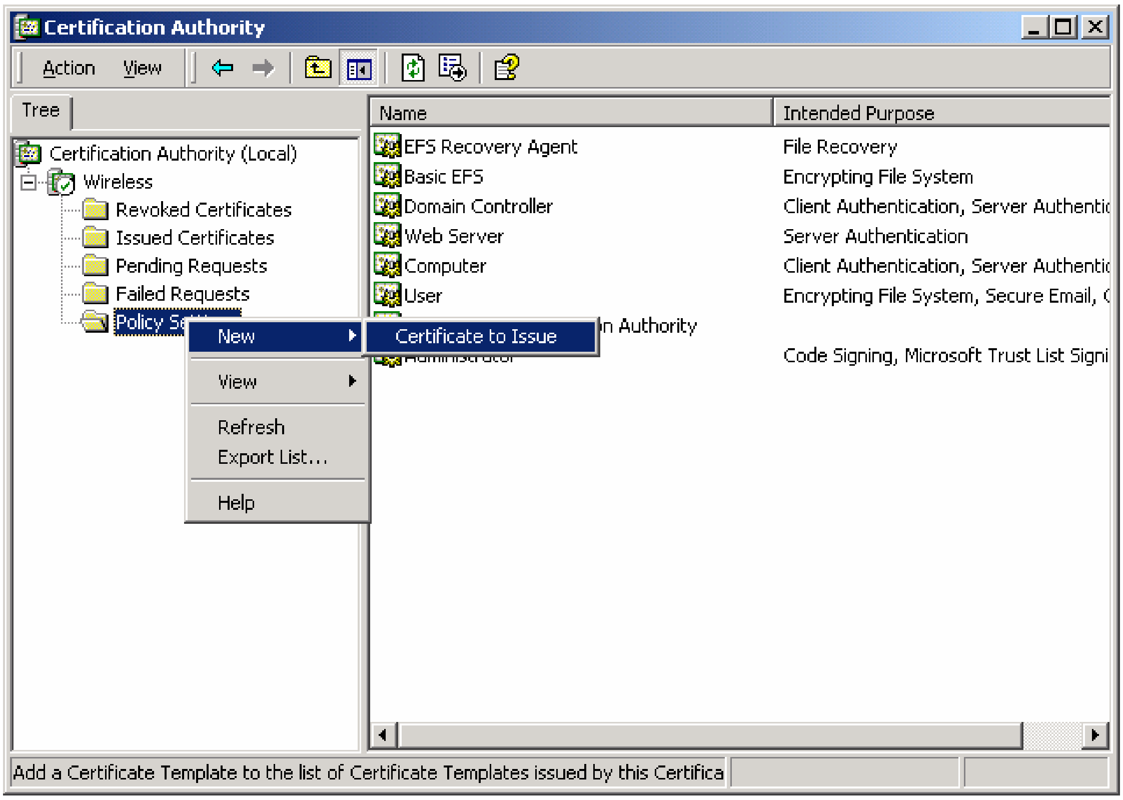
< Back | Next > | Cancel

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

8. You will see “Computer processing Internet information service, you must stop this service to continue”, Press “Yes” to continue.
9. Press “Complete” to finish Wizard.

Step 2: Configuration Certificate Authority

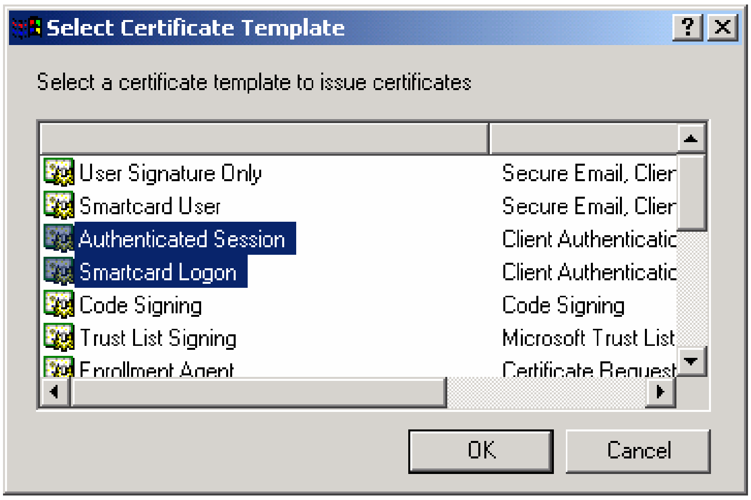
1. Go to ”Start>Program files> System administrative tools>Certificate Authority”.
2. Open “Wireless” (the one you added into your system), right click on the “Policy Setting” select “New”
3. Select “Certificate to Issue”



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
n Authority	
	Code Signing, Microsoft Trust List Signi

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

4. Select ”Authenticated Session” and ”Smartcard Logo n” two Certificate sample by holding down Ctrl key and press “OK” to continue.



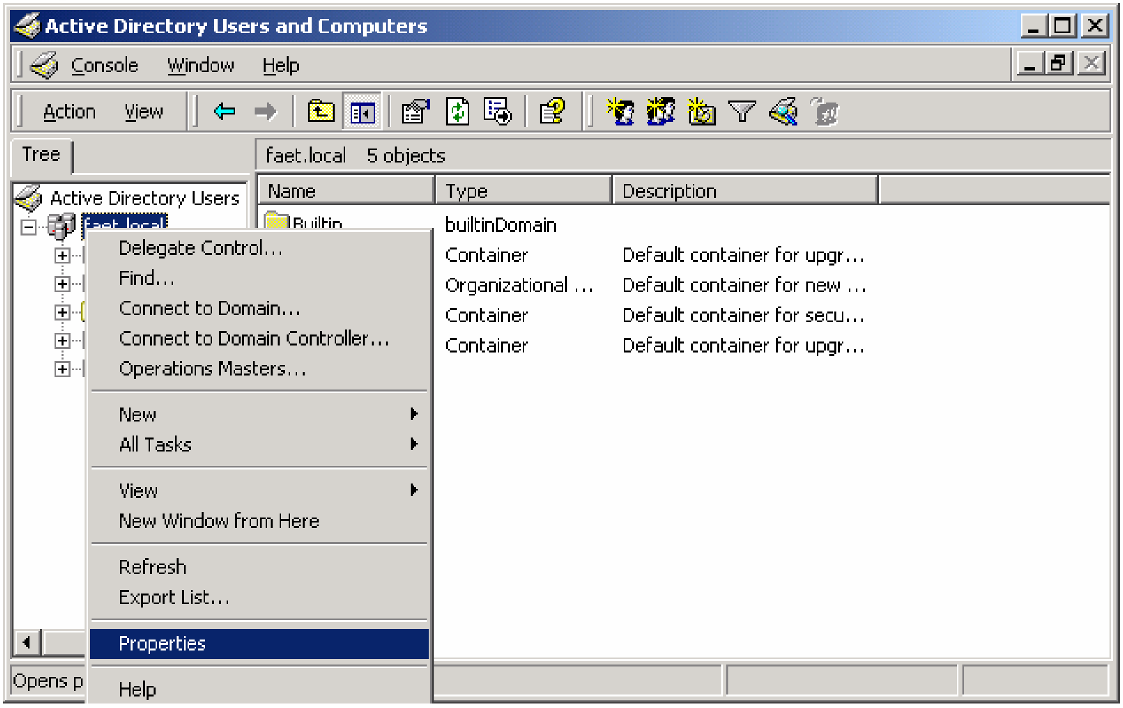
Select Certificate Template

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

5. Go to ”Start> Program> System Administrative Tools> Active Directory Users and Computers”

6. Right Click on your “Domain” and click “Properties”

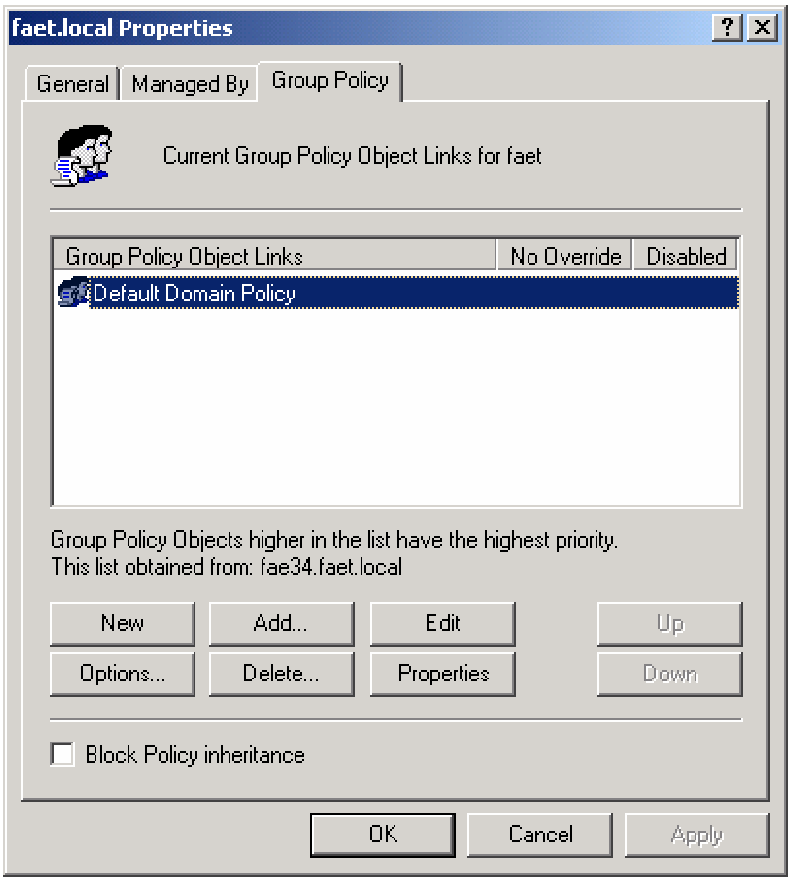


Active Directory Users and Computers

faet.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...

7. Select “Group Policy” tab and tick up “default Domain Policy” click “properties”.



Current Group Policy Object Links for faet

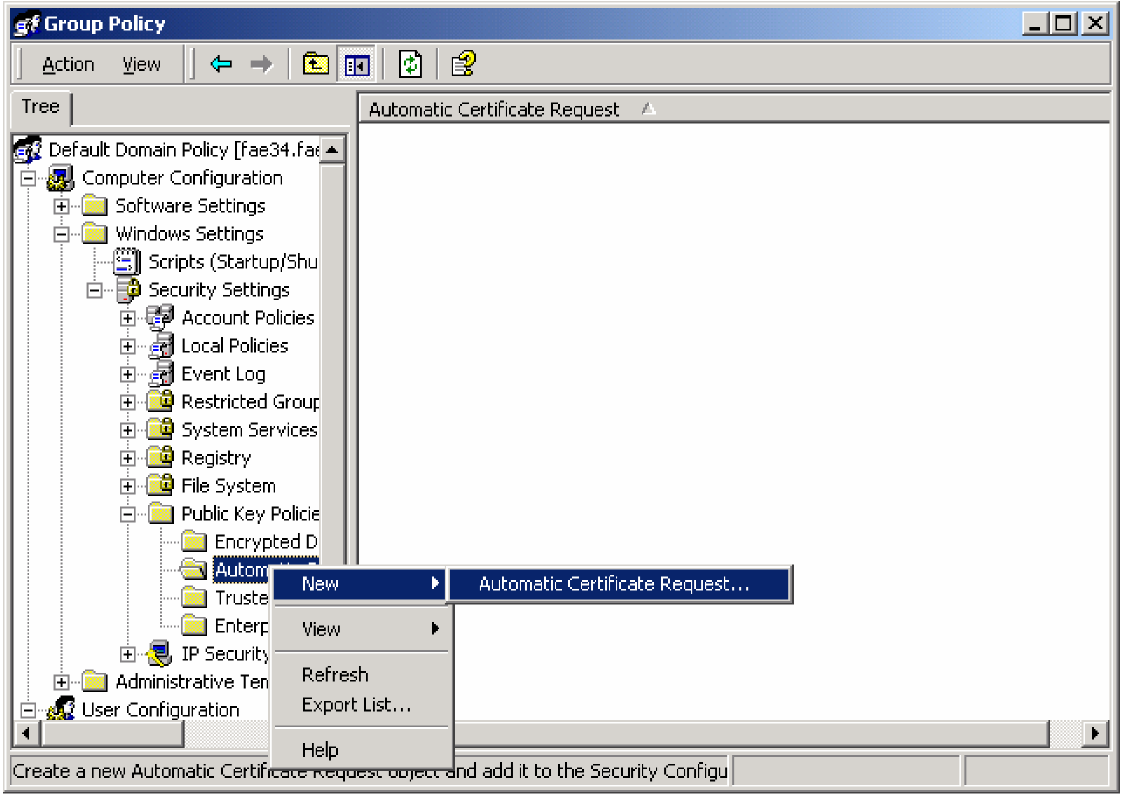
Group Policy Object Links	No Override	Disabled
Default Domain Policy		

Group Policy Objects higher in the list have the highest priority.
This list obtained from: fae34.faet.local

□ Block Policy inheritance

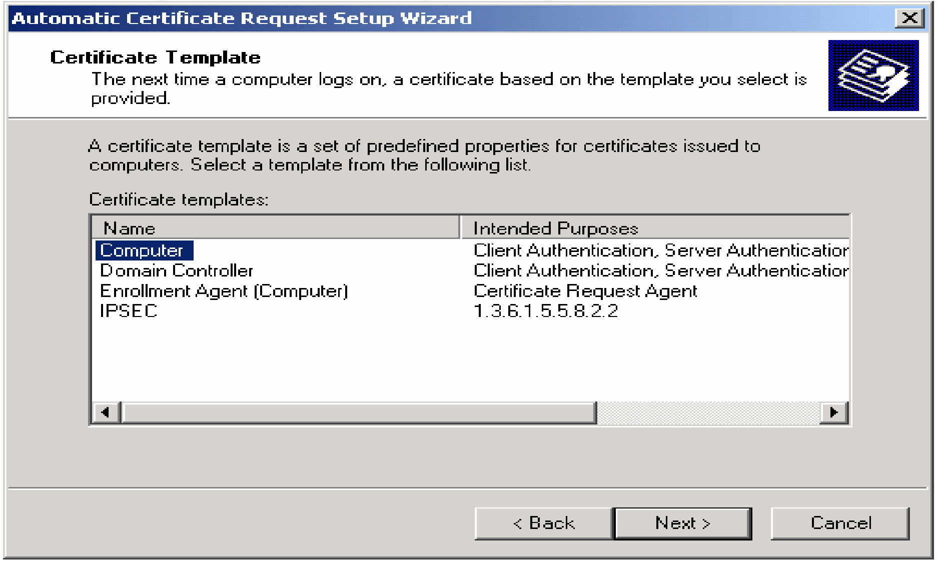
8. Select ”Computer configuration> Security Setting> Public Key Policies>
9. Right Click “Automatic Certificate Request Setting”, select “New” then Click “Automatic Certificate Request……”

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



Create a new Automatic Certificate Request object and add it to the Security Configu

11. Select ”Computer” certificate template and press “Next”.



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.

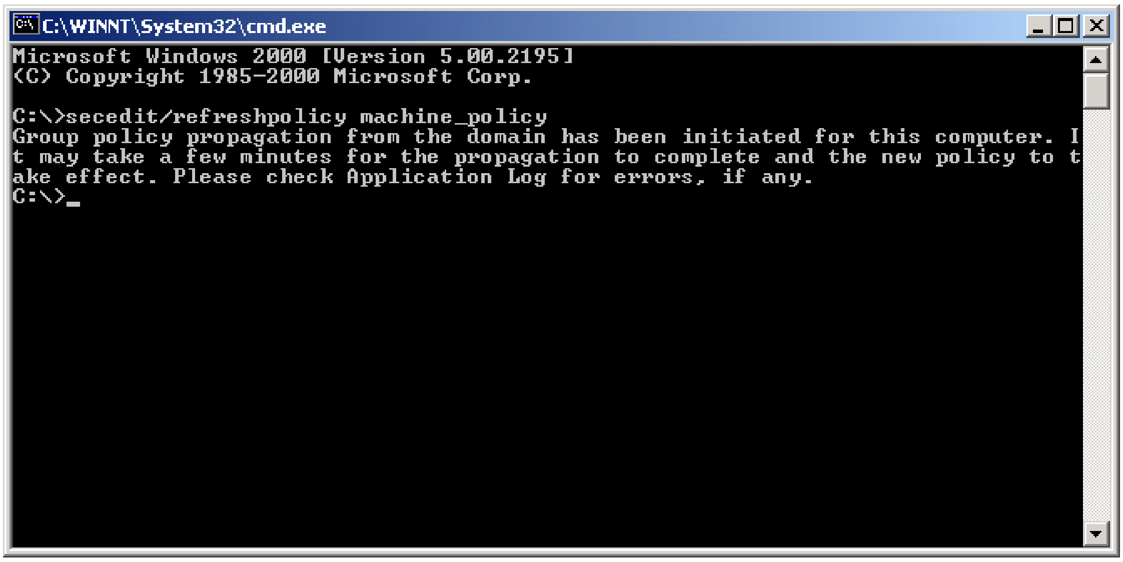
Certificate templates:

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

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”



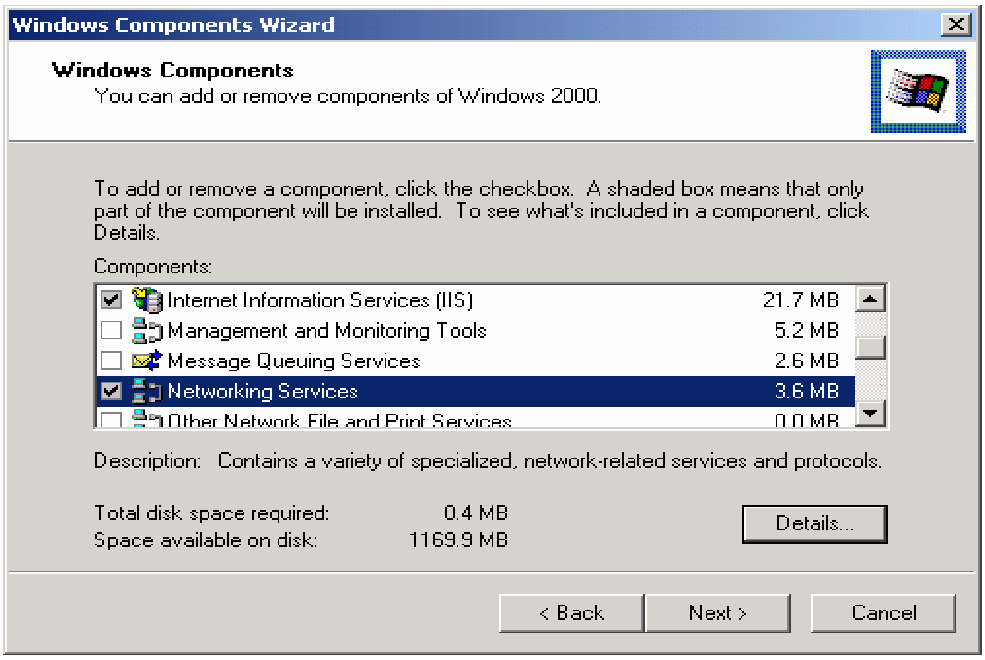
```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

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:\>_
```

15. You can see a message as above.

Step3: Internet Authentication Service (Radius) Configuration

1. Go to ”Start>Control Panel >Add or remove program”
2. Select “Add or Remove Windows Components”, select ”Network Service”



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.

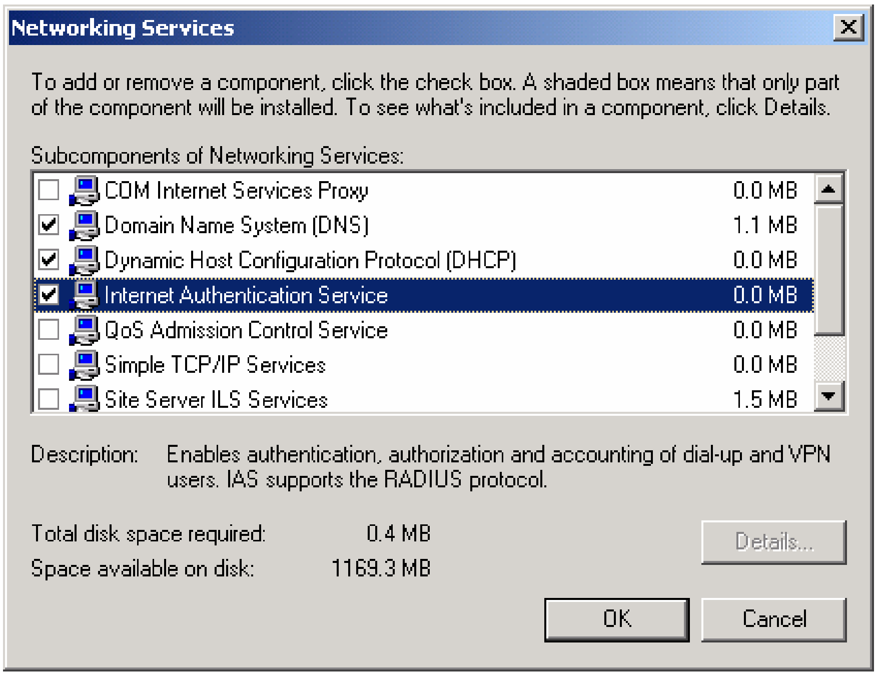
Components:

☑ Internet Information Services (IIS) 21.7 MB
☐ Management and Monitoring Tools 5.2 MB
☐ Message Queuing Services 2.6 MB
☑ Networking Services 3.6 MB
☐ Other Network File and Print Services 0.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.4 MB
Space available on disk: 1169.9 MB

3. Press “Details…” and select ”Internet Authentication Service”



Networking Services

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:

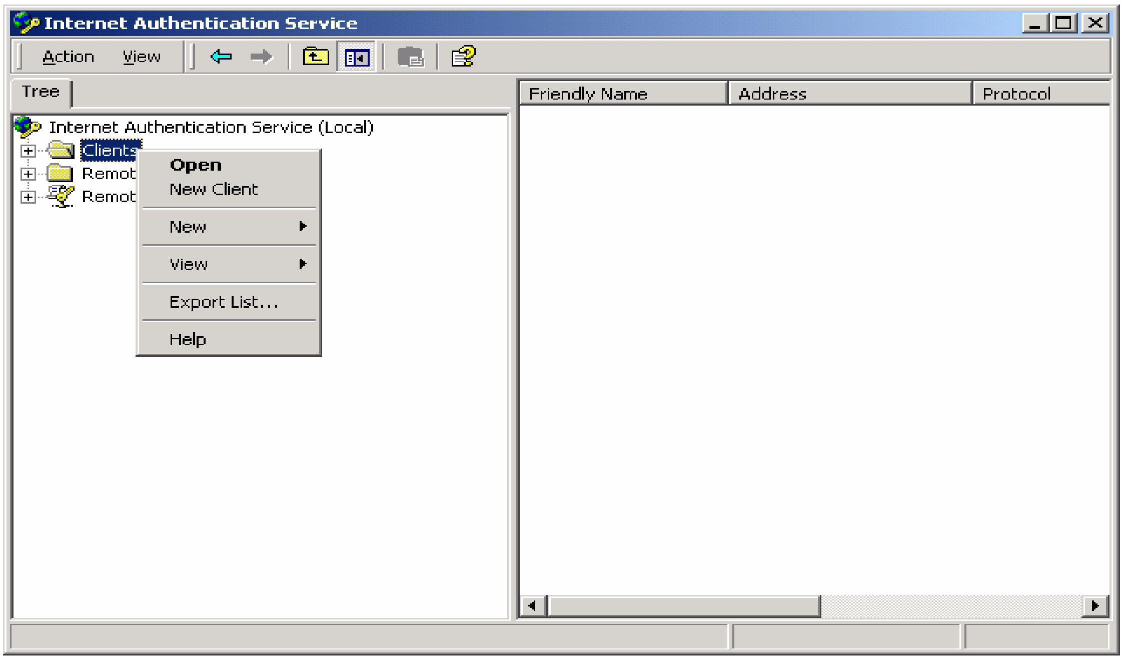
□	COM Internet Services Proxy	0.0 MB
☑	Domain Name System (DNS)	1.1 MB
☑	Dynamic Host Configuration Protocol (DHCP)	0.0 MB
☑	Internet Authentication Service	0.0 MB
□	QoS Admission Control Service	0.0 MB
□	Simple TCP/IP Services	0.0 MB
□	Site Server ILS Services	1.5 MB

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

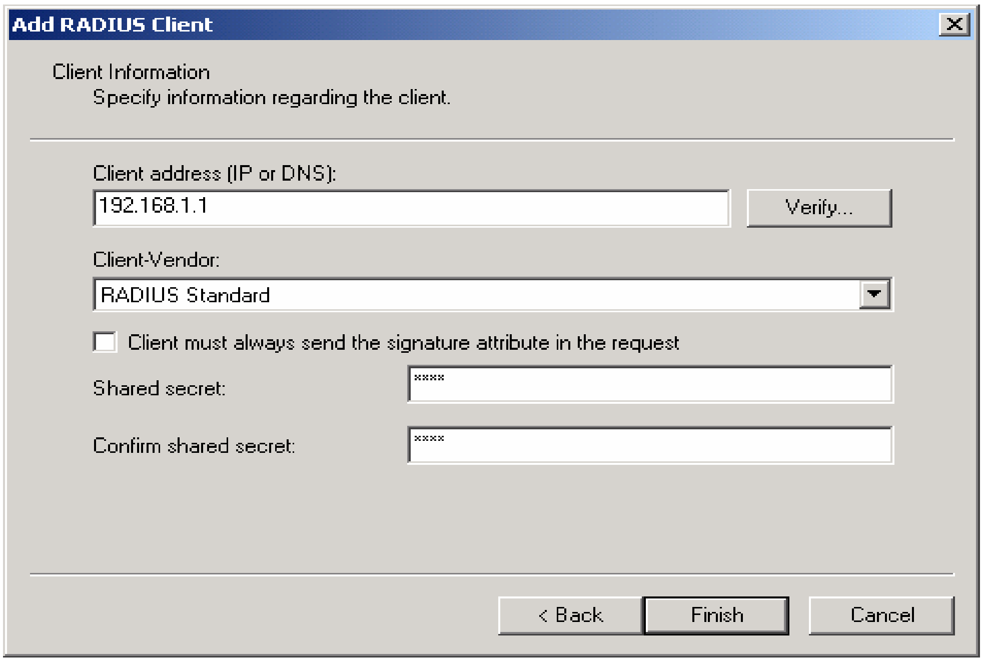
Total disk space required: 0.4 MB

Space available on disk: 1169.3 MB

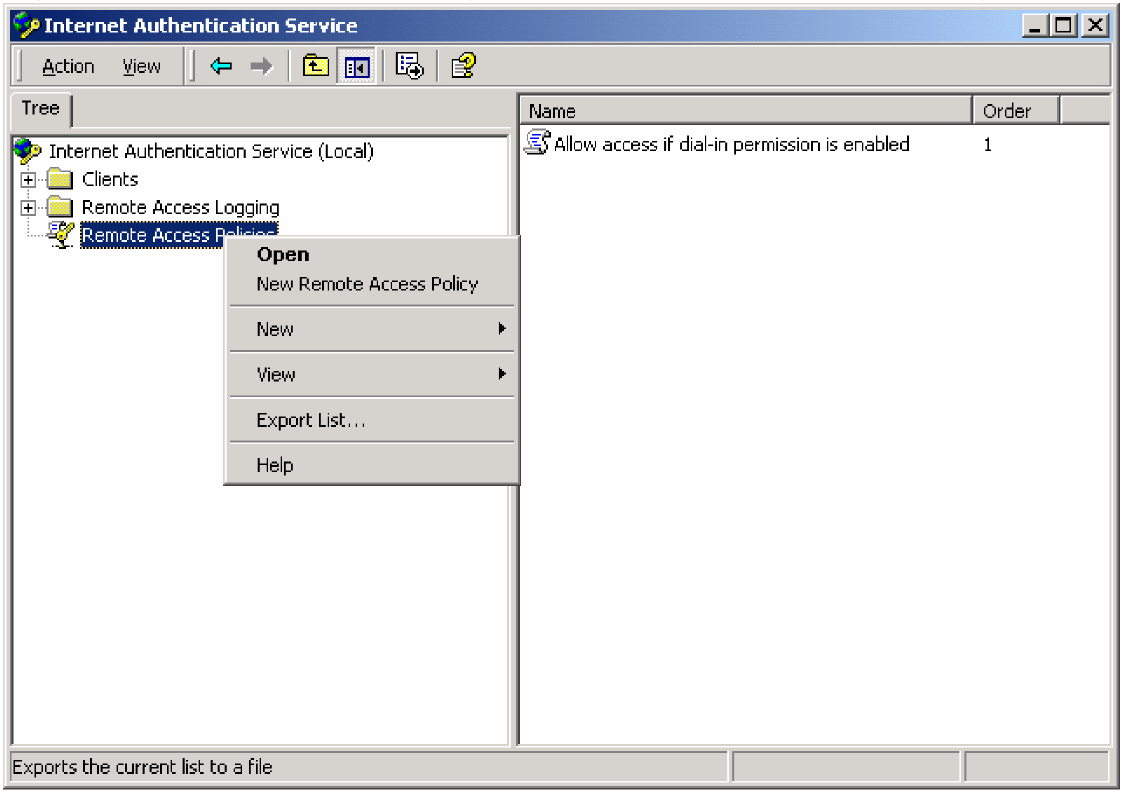
4. Go to ”Start>Programs>System Administrative Tools>Internet Authentication Service”.
5. Right Click on “Client” click “New Client”



6. Put a name to represent your Access Point and press “Next”.

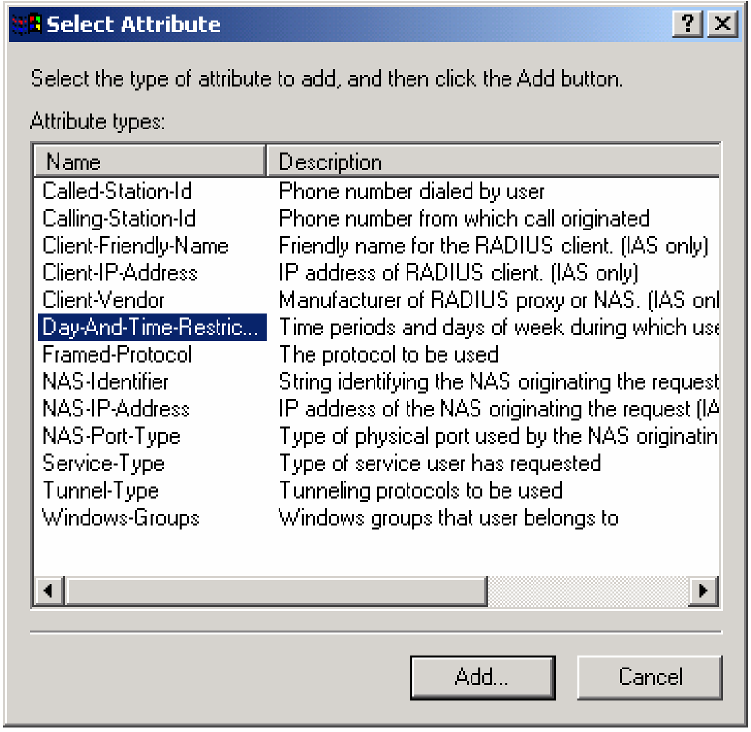


7. Key in a share key for this Access Point.
8. Press "Finish" to complete.
9. Right click on "Remote Access Policy" and select "New Remote Access Policy"


Internet Authentication Service
Action
View
Tree
Internet Authentication Service (Local)
Clients
Remote Access Logging
Remote Access Policies
Open
New Remote Access Policy
New
View
Export List...
Help
Name
Order
Allow access if dial-in permission is enabled
1
Exports the current list to a file

10. Type a name for new policy, press "Next".

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



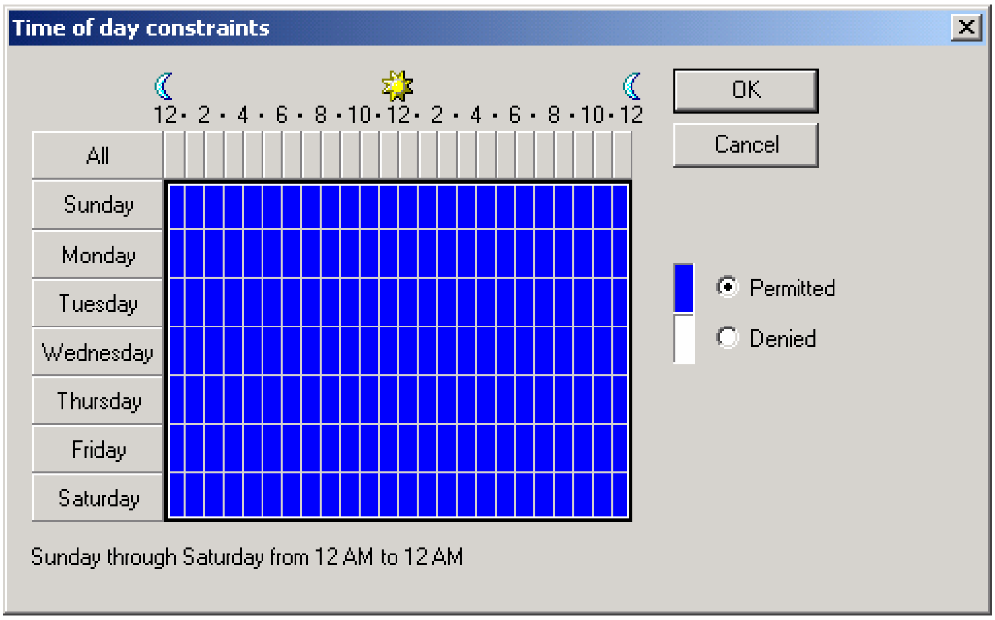
Select Attribute

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

12. Tick “Permitted” and select this service operation time.



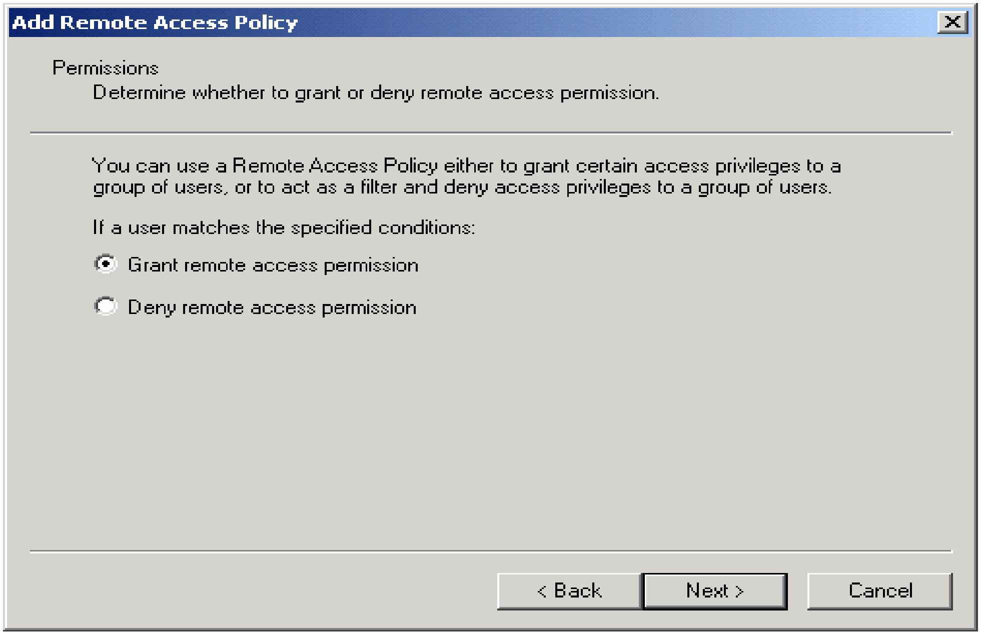
Time of day constraints

● Permitted

○ Denied

Sunday through Saturday from 12 AM to 12 AM

13. Tick “Grant remote access permission” and click “Next”.



Add Remote Access Policy

Permissions
Determine whether to grant or deny remote access permission.

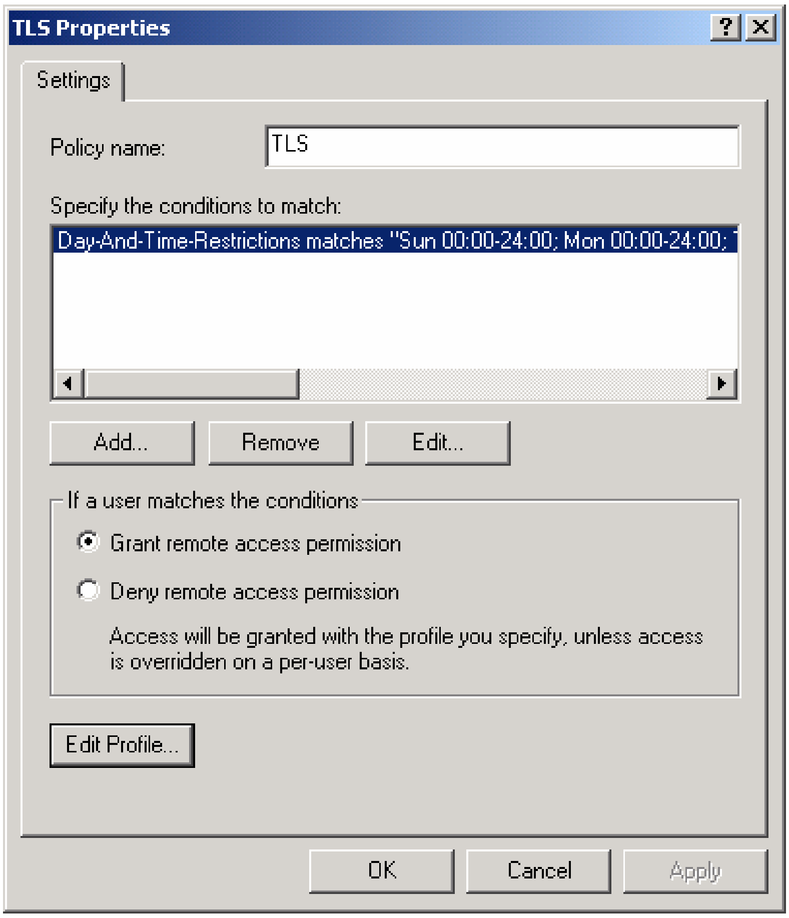
You can use a Remote Access Policy either to grant certain access privileges to a group of users, or to act as a filter and deny access privileges to a group of users.

If a user matches the specified conditions:

● Grant remote access permission

○ Deny remote access permission

14. Press ”Edit Profile”



TLS Properties

Settings

Policy name: TLS

Specify the conditions to match:

Day-And-Time-Restrictions matches "Sun 00:00-24:00; Mon 00:00-24:00;

If a user matches the conditions

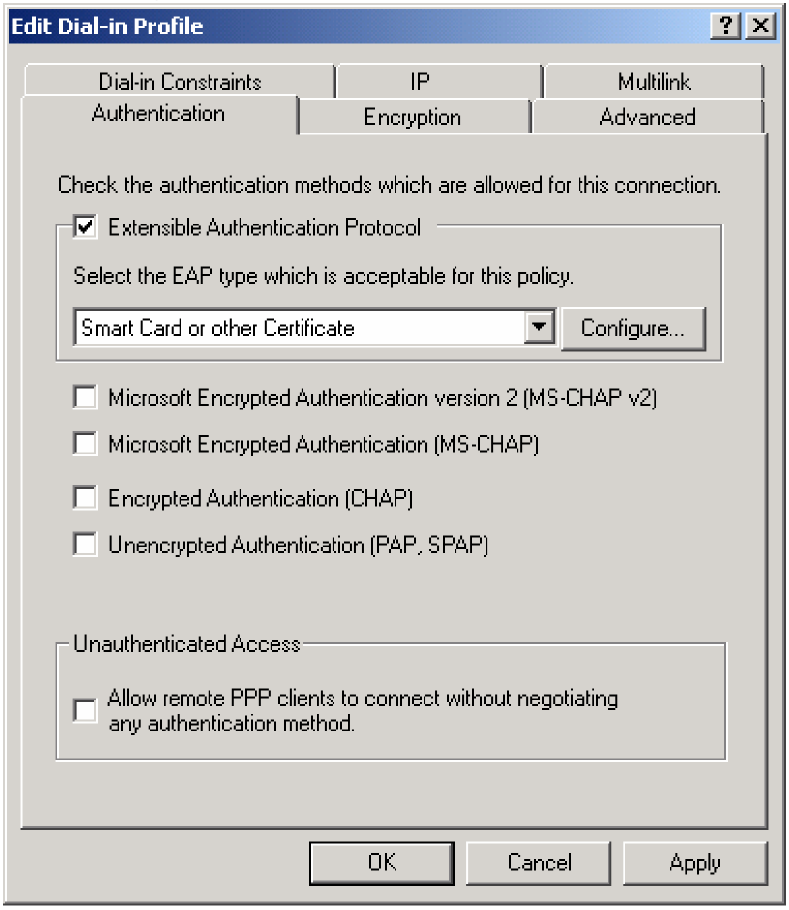
● Grant remote access permission

○ Deny remote access permission

Access will be granted with the profile you specify, unless access is overridden on a per-user basis.

15. Select Authentication method; tick ”Extensible Authentication Protocol” up and select “Smart Card or other Certification” in Authentication. Press “OK” to complete configuration.

Note: If you need other authentication method please ticks up here.



Edit Dial-in Profile

Dial-in Constraints | IP | Multilink | Authentication | Encryption | Advanced

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 ▾ Configure...

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

□ Microsoft Encrypted Authentication (MS-CHAP)

□ Encrypted Authentication (CHAP)

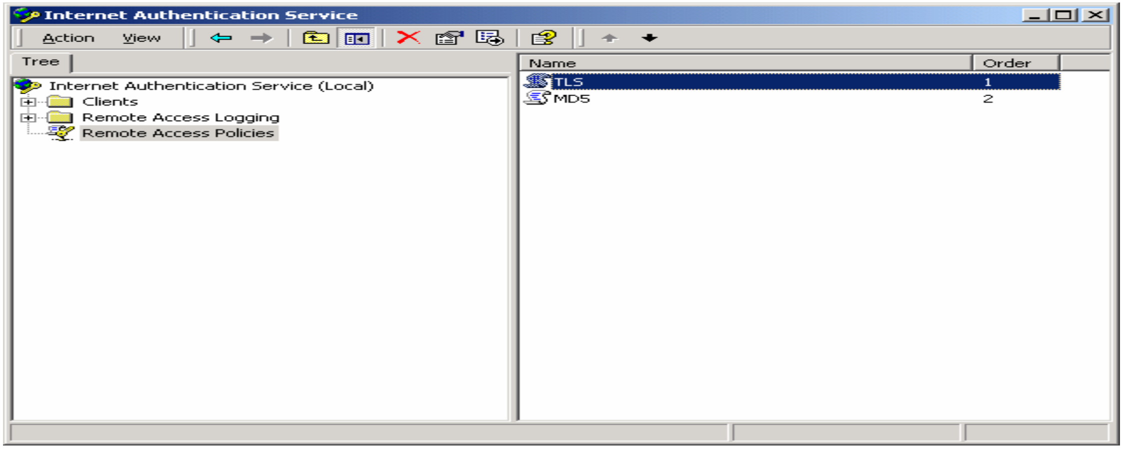
□ Unencrypted Authentication (PAP, SPAP)

Unauthenticated Access

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

OK Cancel Apply

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



Internet Authentication Service

Action View

Tree

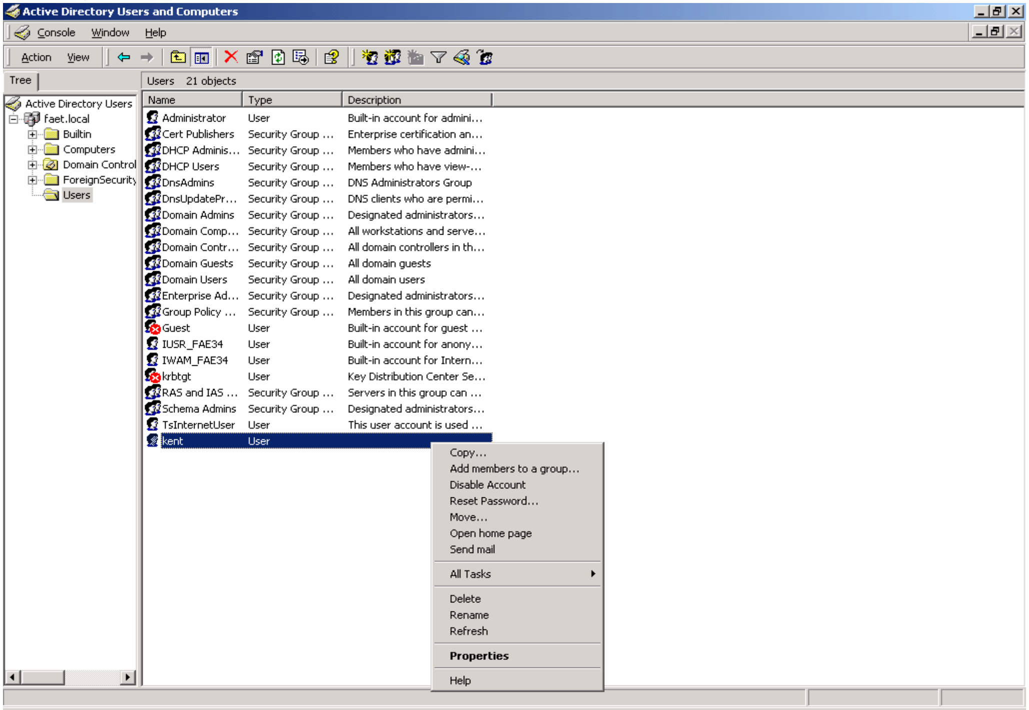
- Internet Authentication Service (Local)
  - Clients
  - Remote Access Logging
  - Remote Access Policies

Name	Order
TLS	1
MD5	2

17. Go to “Start> Program>System Administrative tools> Active Directory Users and

Computers”

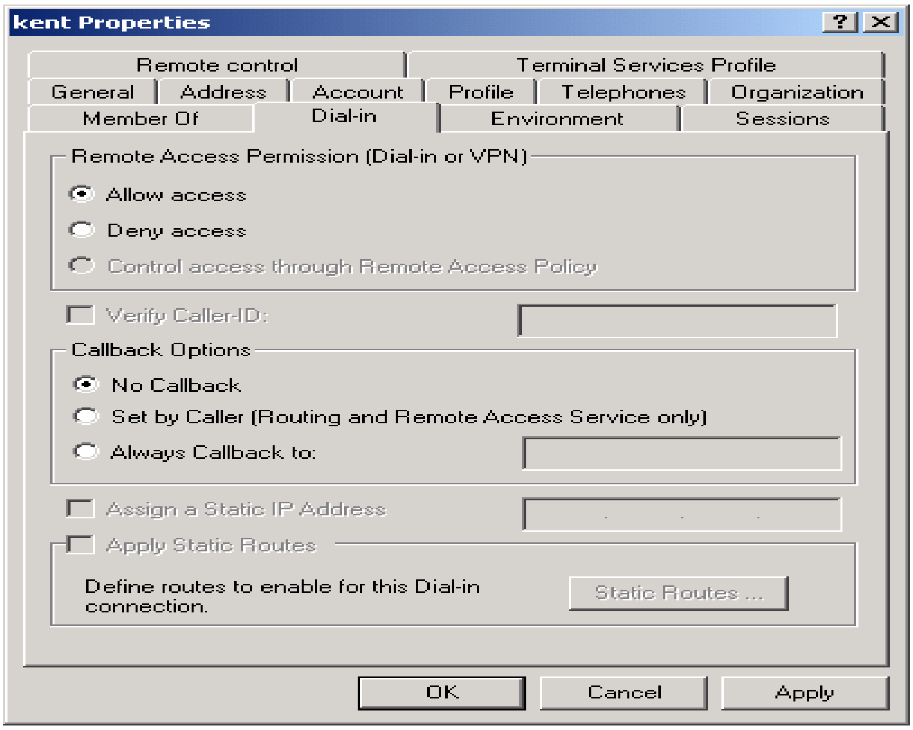
18. Right click a user who needs this service.



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_FAE34	User	Built-in account for anony...
IWAM_FAE34	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 ...
kent	User	

19. Select “Dial-in”, Tick “Allow Access” in Remote Access Permission press “OK” to complete Configuration.



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)

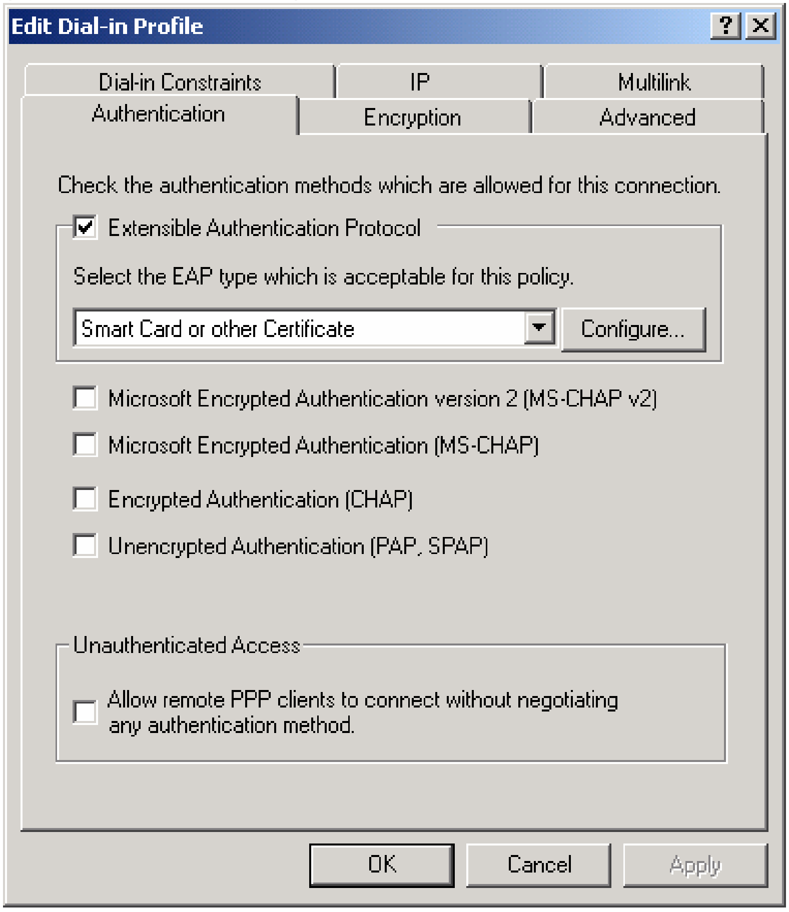
○ Always Callback to:

□ Assign a Static IP Address

□ Apply Static Routes

Define routes to enable for this Dial-in connection.

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



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.

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)

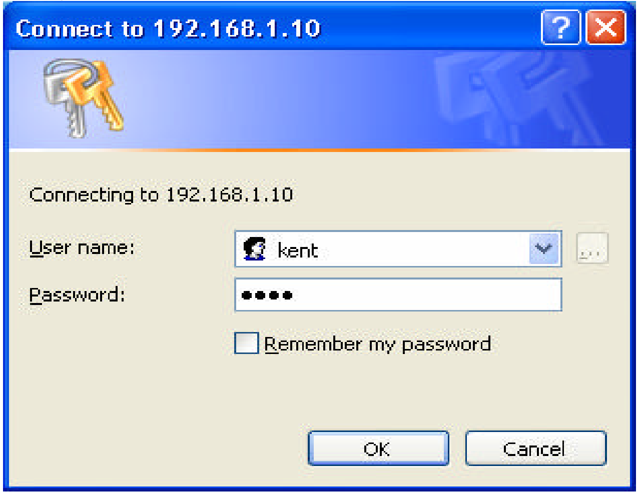
Unauthenticated Access

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

Part 3-2: 802.1x TLS Logon

Step 1: Get a CA

1. Connect your computer to a network, which can connect to RADIUS Server (How ever wired or wireless connection, if you do use wireless connection please turn all security method off first otherwise you will fail on this step)
2. Open you browser (For Example IE), put "RADIUS Server IP/certsrv"(for example "192.168.1.10/certsrv"). Please make sure IIS service of your Windows 2000 server is turn on.
3. Server will return a message for ID/password request. Please put your ID/password (you had setup this ID in previous step).



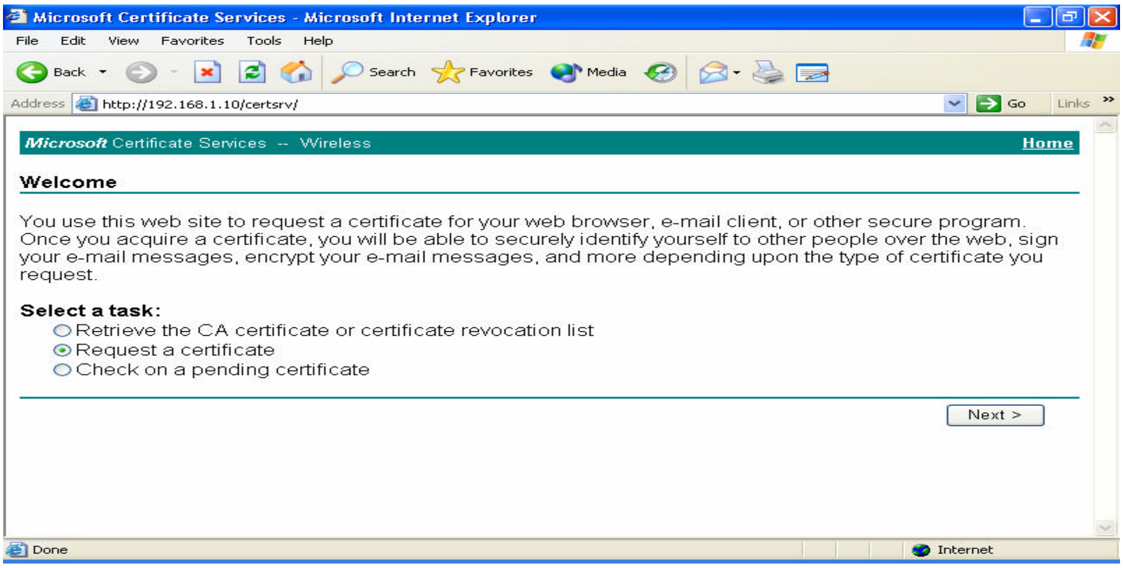
Connecting to 192.168.1.10

User name: kent

Password: ●●●●

□ Remember my password

4. A Microsoft Certificate Service --- Wireless page jump out, Select "Request a Certificate" Press "Next.


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

Microsoft Certificate Services -- Wireless **Home**

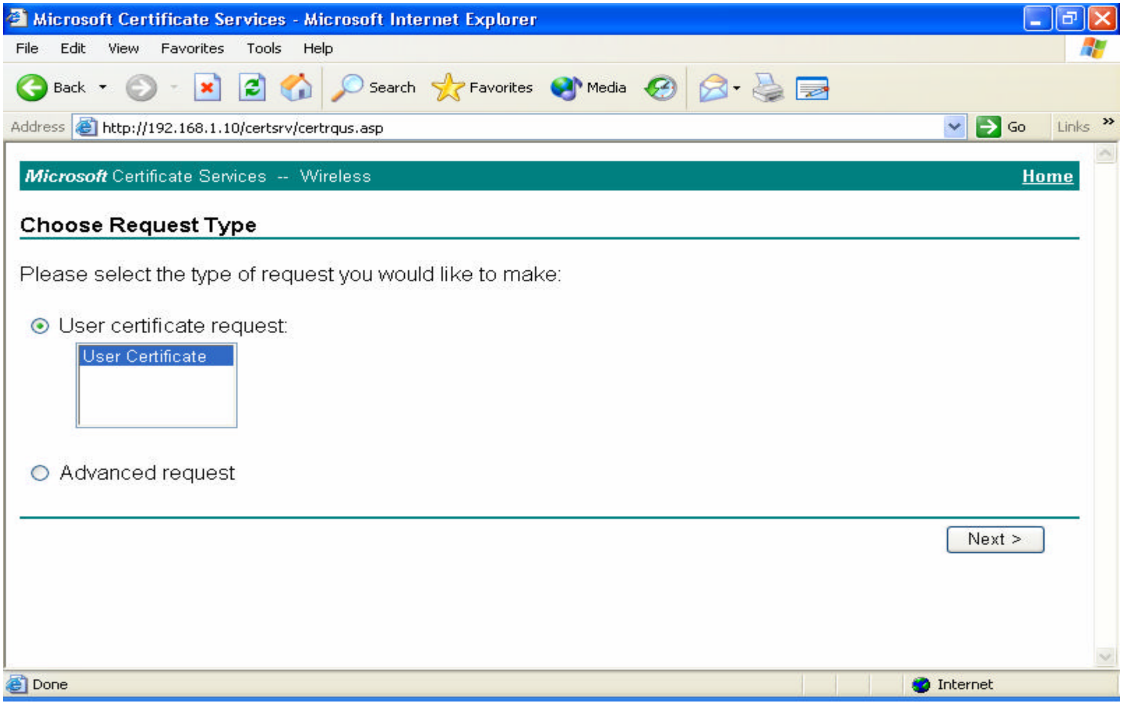
Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

○ Retrieve the CA certificate or certificate revocation list
● Request a certificate
○ Check on a pending certificate

5. Select ”User certificate request” press “Next”.



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

Microsoft Certificate Services -- Wireless **Home**

Choose Request Type

Please select the type of request you would like to make:

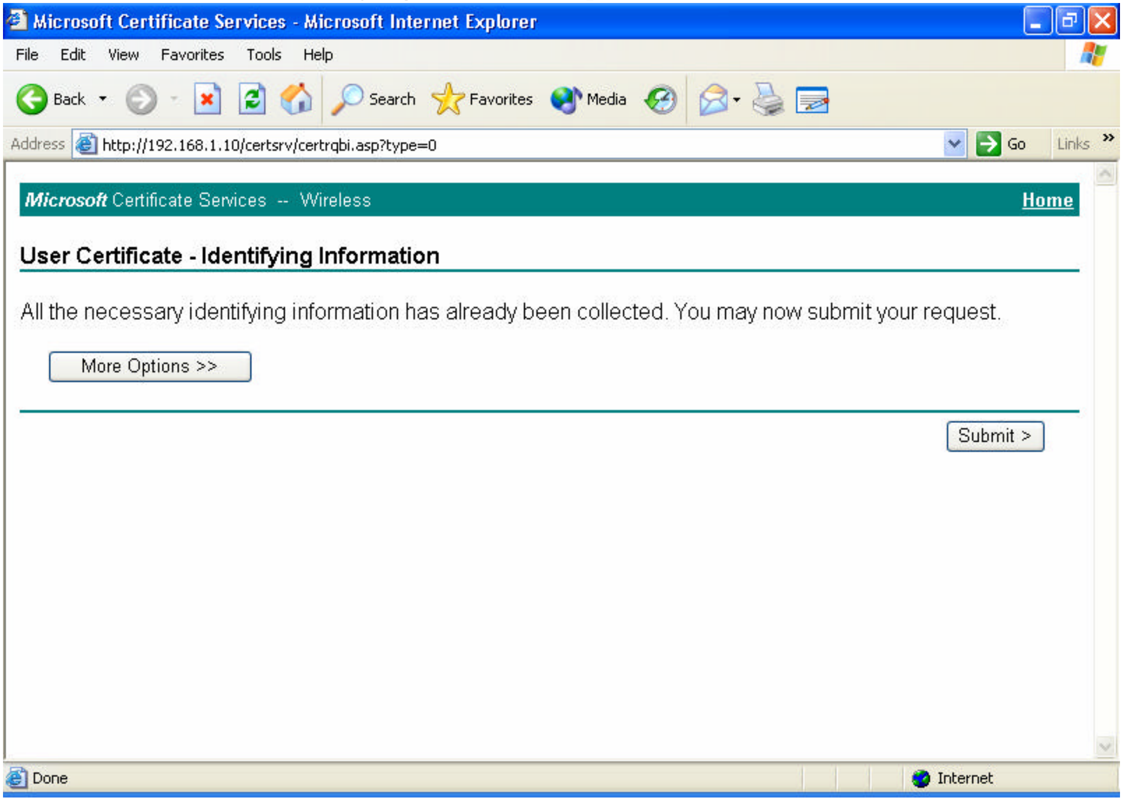
● User certificate request:

User Certificate

○ Advanced request

Next >

6. User Certificate – Identifying Information, press “Submit”.



Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.10/certsrv/certrqbi.asp?type=0 Go Links

Microsoft Certificate Services -- Wireless **Home**

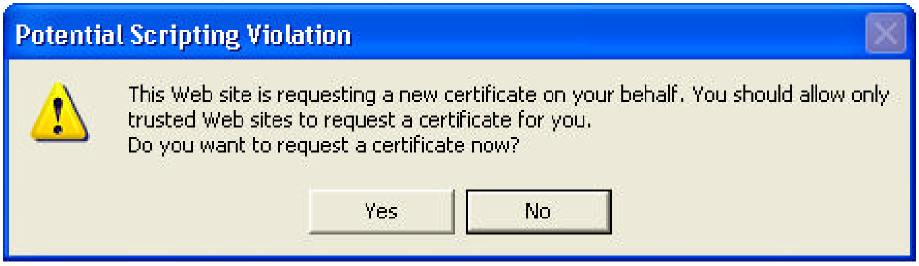
User Certificate - Identifying Information

All the necessary identifying information has already been collected. You may now submit your request.

More Options >>

Submit >

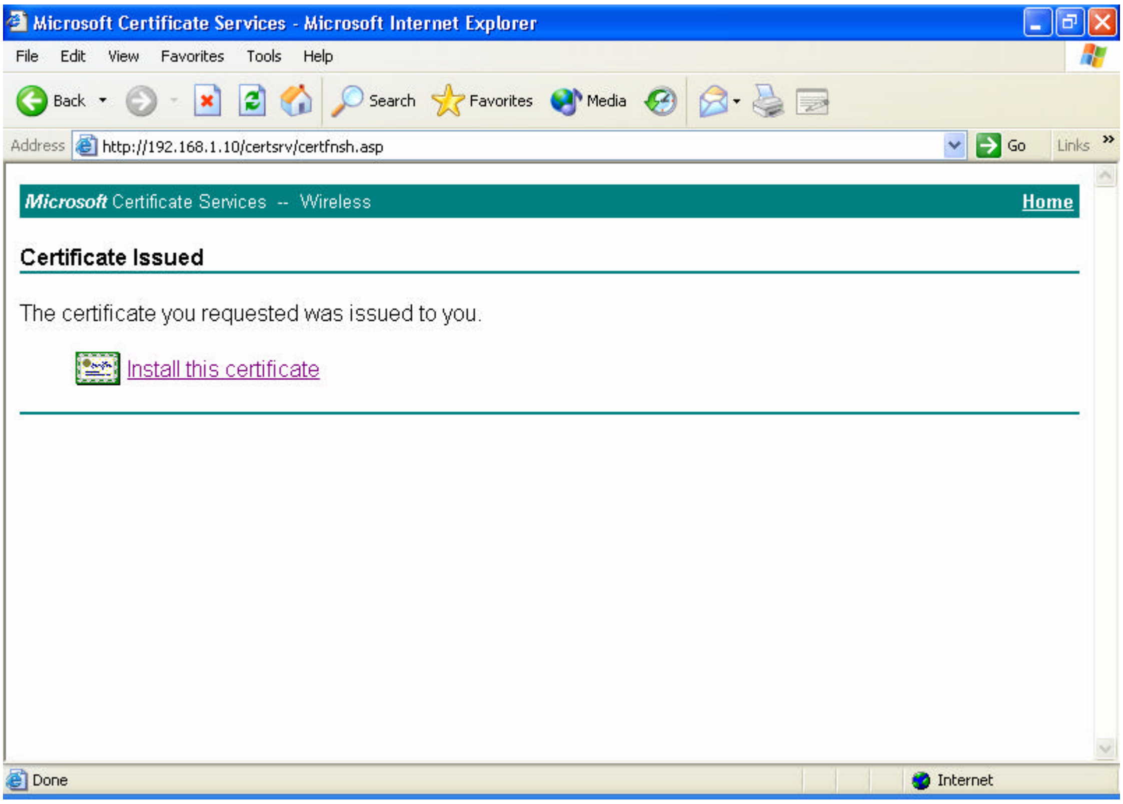
7. A CA warning POP message jump out, press ”Yes”.



Potential Scripting Violation

This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you.
Do you want to request a certificate now?

8. Click “Install this certificate”



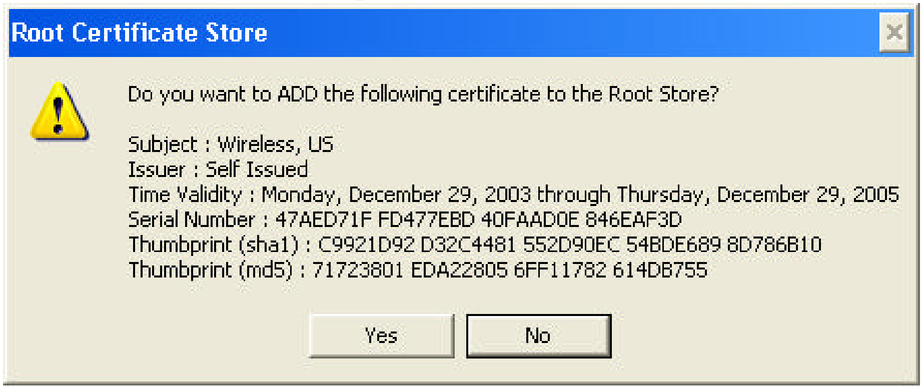
Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.10/certsrv/certfnsh.asp
Go Links
Microsoft Certificate Services -- Wireless
Home
Done
Internet

Certificate Issued

The certificate you requested was issued to you.

Install this certificate

9. Confirm to add this CA, press “Yes”.

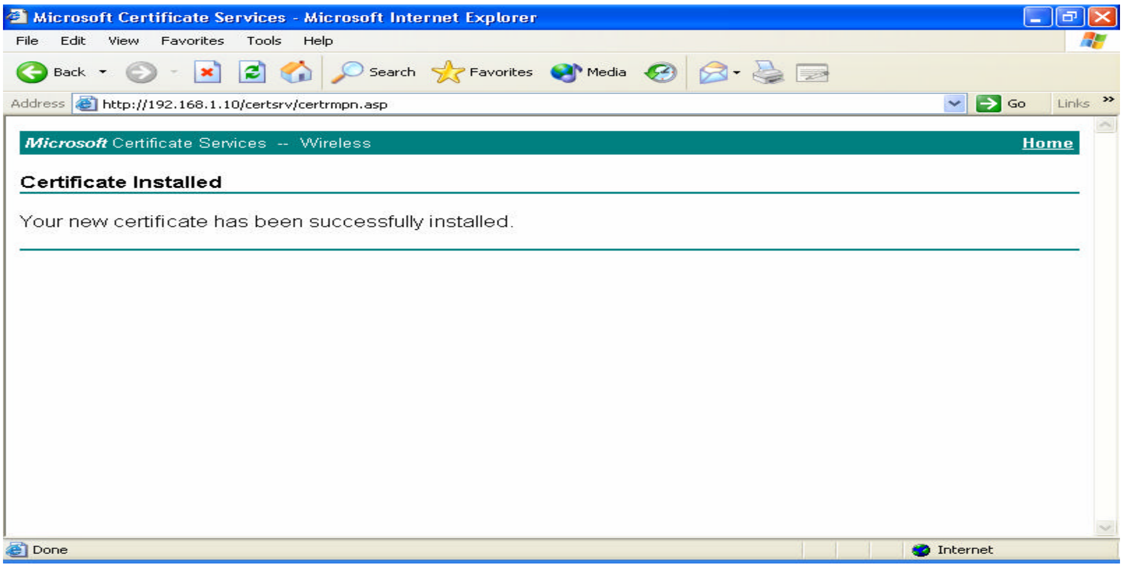


Root Certificate Store

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

Subject : Wireless, US
Issuer : Self Issued
Time Validity : Monday, December 29, 2003 through Thursday, December 29, 2005
Serial Number : 47AED71F FD477EBD 40FAAD0E 846EAF3D
Thumbprint (sha1) : C9921D92 D32C4481 552D90EC 54BDE689 8D786B10
Thumbprint (md5) : 71723801 EDA22805 6FF11782 614DB755

10. Certificate Installed.



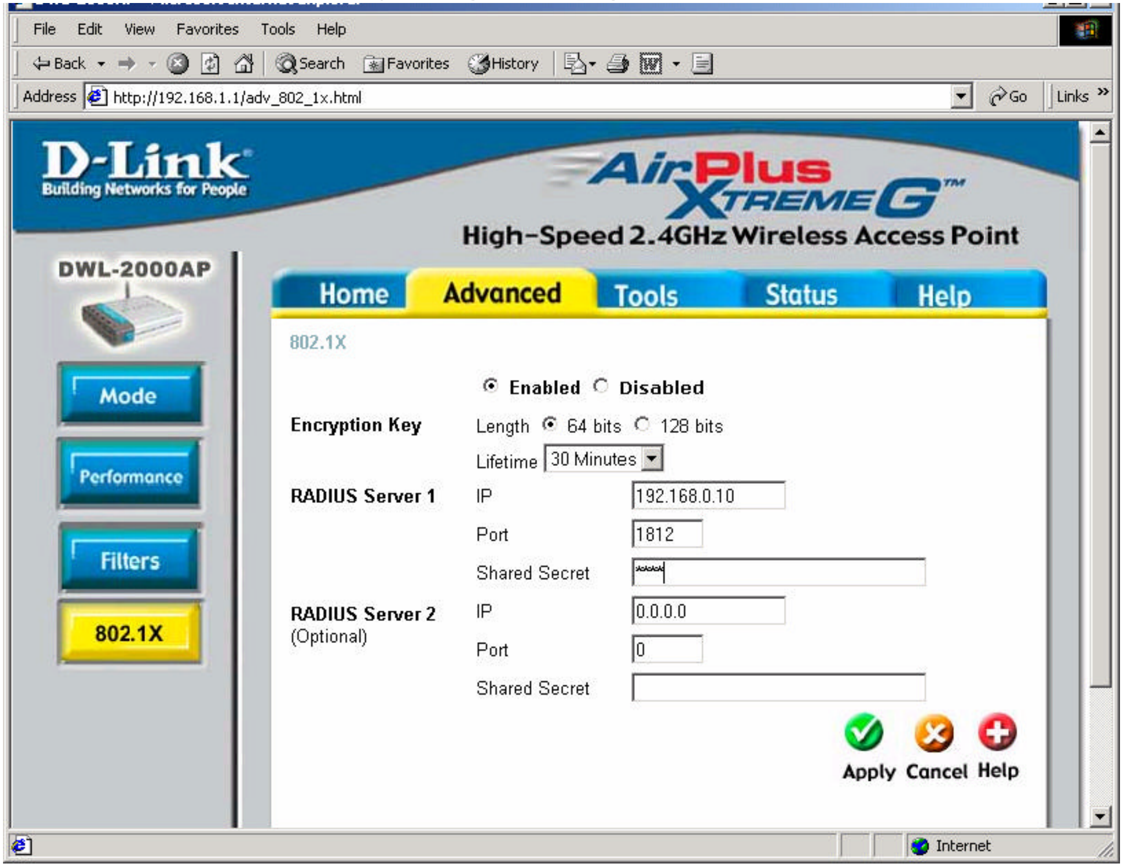
Microsoft Certificate Services -- Wireless

Certificate Installed

Your new certificate has been successfully installed.

Step 2: Configuration Access Point

1. Open Access Point Security configuration page



Address: http://192.168.1.1/adv_802_1x.html

D-Link Building Networks for People

AirPlus XtremeG High-Speed 2.4GHz Wireless Access Point

DWL-2000AP

802.1X

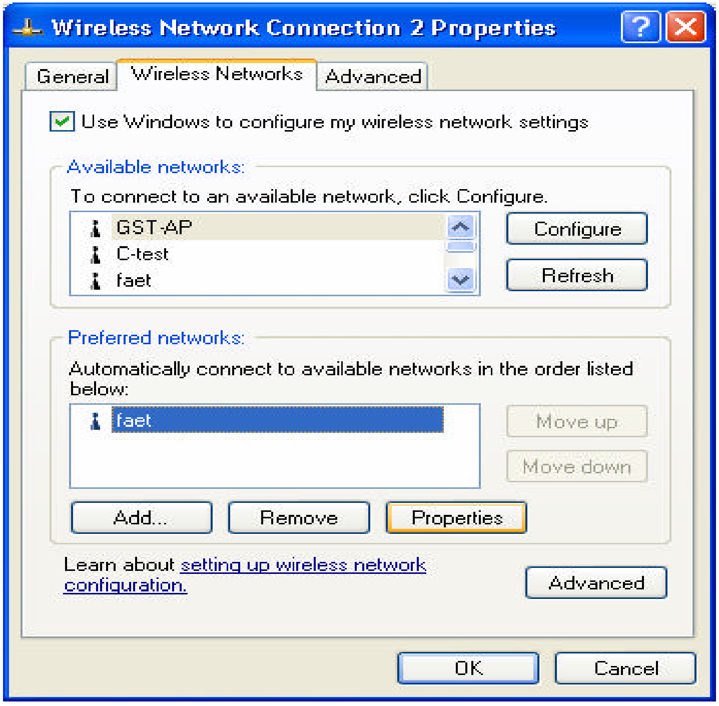
	● Enabled ○ Disabled	
Encryption Key	Length ● 64 bits ○ 128 bits	
	Lifetime	30 Minutes
RADIUS Server 1	IP	192.168.0.10
	Port	1812
	Shared Secret	****
RADIUS Server 2 (Optional)	IP	0.0.0.0
	Port	0
	Shared Secret	

2. Select “802.1x”
3. Configuration this page
   - Lifetime: A period to change Key
   - Length: Encryption Length
   - IP: RADIUS Server IP
   - Port: Service Port (Standard RADIUS use port 1812)
   - Shared Secret: Share key on RADIUS server (the one you had set for this AP)

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

Step 3: 802.1x Connection

1. Here we will use Windows XP Wireless Zero Configuration Utility to be the sample connection, please be noted the page might bit different in different Windows XP version.
2. Right click “My Network Place” on your desktop and click “Properties” (or go to “Start/ Settings/ Network” or double click a network icon which represents your wireless network on system tray where right down your screen).
3. Select your Wireless LAN Card right clicks and selects “Properties”.
4. Click “Wireless Network”.
5. Select the Access Point which you going to connect and click “Configuration” on its right.



Wireless Network Connection 2 Properties

☑ Use Windows to configure my wireless network settings

Available networks:

To connect to an available network, click Configure.

GST-AP
C-test
faet

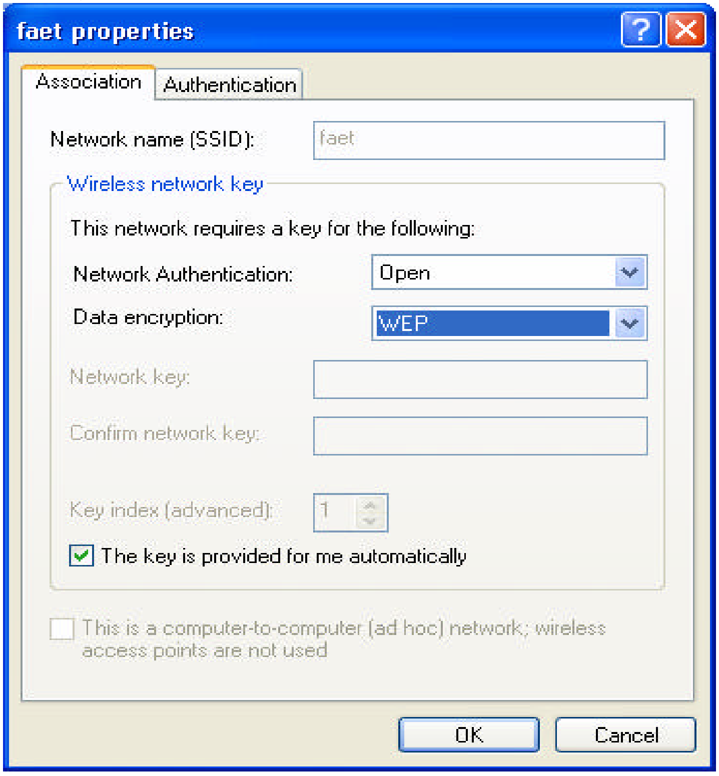
Preferred networks:

Automatically connect to available networks in the order listed below:

faet

Learn about setting up wireless network configuration.

6. Select”OPEN System” on Network Authentication, uses WEP encryption Tick “The key is provided for me automatically” up.



Network name (SSID): faet

Wireless network key

This network requires a key for the following:

Network Authentication: Open

Data encryption: WEP

Network key:

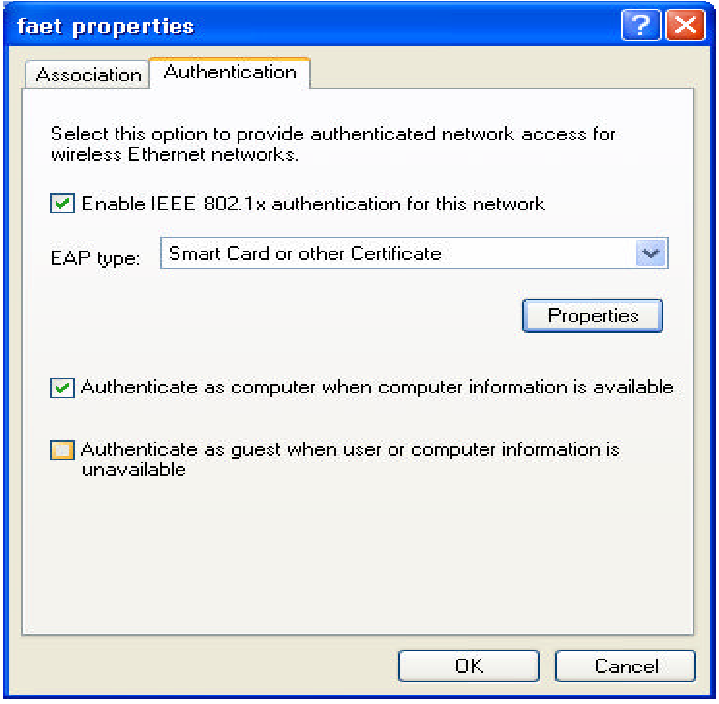
Confirm network key:

Key index (advanced): 1

☑ The key is provided for me automatically

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

7. Select “Authentication” page. Tick “Enabled IEEE 802.1xAuthentication for this Network”, EAP Type selects ”Smart Card or other certificate”. Press “OK”.



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

☑ Enable IEEE 802.1x authentication for this network

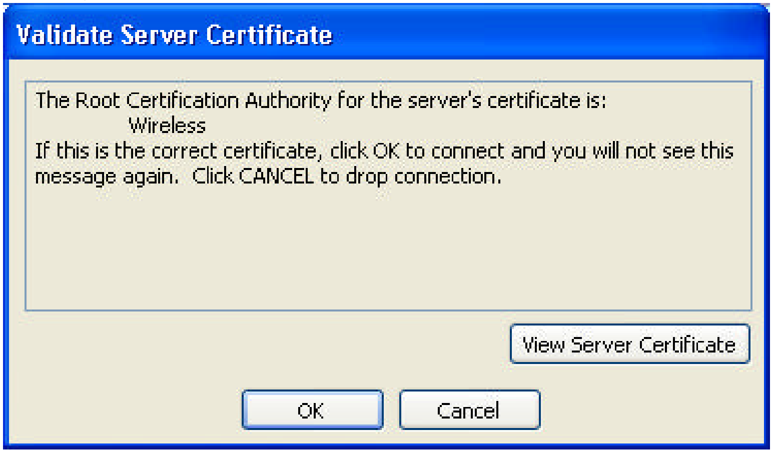
EAP type: Smart Card or other Certificate

☑ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

8. When Station connected to AP, a connection process request will right on your screen. Click it you can see a pop window as below (If there has more than a CA on your system you will see a CA selection screen first)

Note: New Windows version can handle it automatically; you might see the latest step directly.



Validate Server Certificate

The Root Certification Authority for the server's certificate is:
Wireless
If this is the correct certificate, click OK to connect and you will not see this message again. Click CANCEL to drop connection.

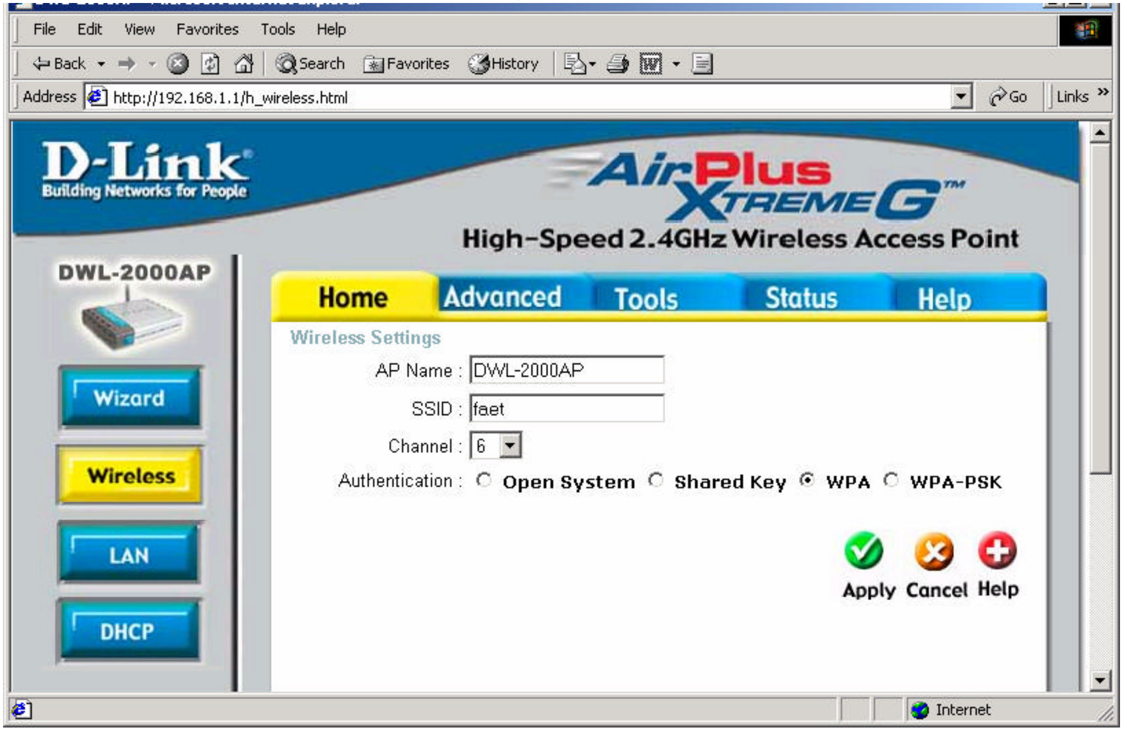
Part 3-3: WPA Logon

Step 1: Request CA

Please refer the way 802.1x request CA

Step 2: AP Configuration

1. Open security web page on your Access Point.
2. Select WPA on this page, press “Apply”.


File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.1.1/h_wireless.html
Go Links
D-Link
Building Networks for People
AirPlus XTREME G™
High-Speed 2.4GHz Wireless Access Point
DWL-2000AP
Wizard
Wireless
LAN
DHCP
Home
Advanced
Tools
Status
Help
Wireless Settings
Apply
Cancel
Help
Internet

AP Name : DWL-2000AP

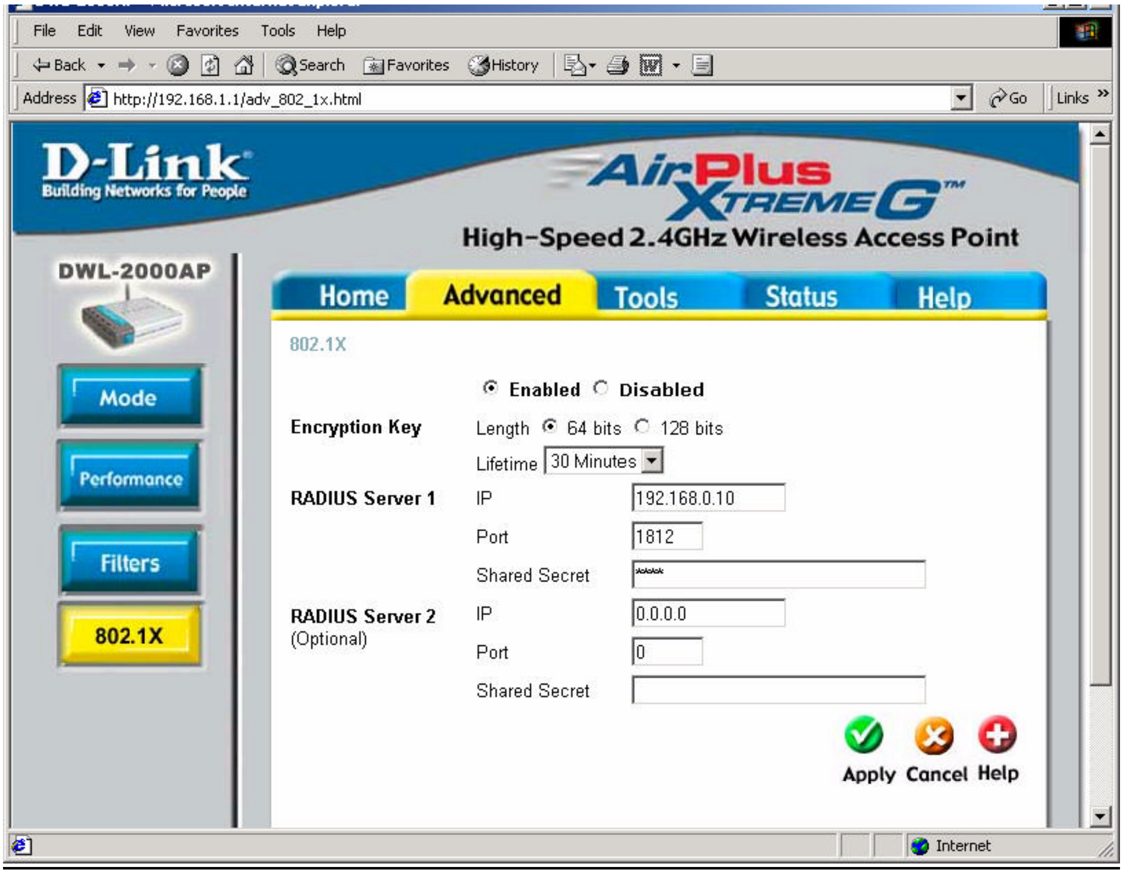
SSID : faet

Channel : 6

Authentication : ○ Open System ○ Shared Key ● WPA ○ WPA-PSK

3. Go 802.1x Configuration page
   - Lifetime: A period to change Key
   - Length: Encryption Length
   - IP: RADIUS Server IP
   - Port: Service Port (Standard RADIUS use port 1812)
   - Shared Secret: Share key on RADIUS server (the one you had set for this AP)

Note: If you have a backup RADIUS server, please set server 2 up as well.


File Edit View Favorites Tools Help
Back Search Favorites History
Go Links
D-Link Building Networks for People
AirPlus XtremeG™
High-Speed 2.4GHz Wireless Access Point
DWL-2000AP
Home
Advanced
Tools
Status
Help
Mode
Performance
Filters
802.1X
Apply
Cancel
Help
Internet

Address http://192.168.1.1/adv_802_1x.html

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 ****

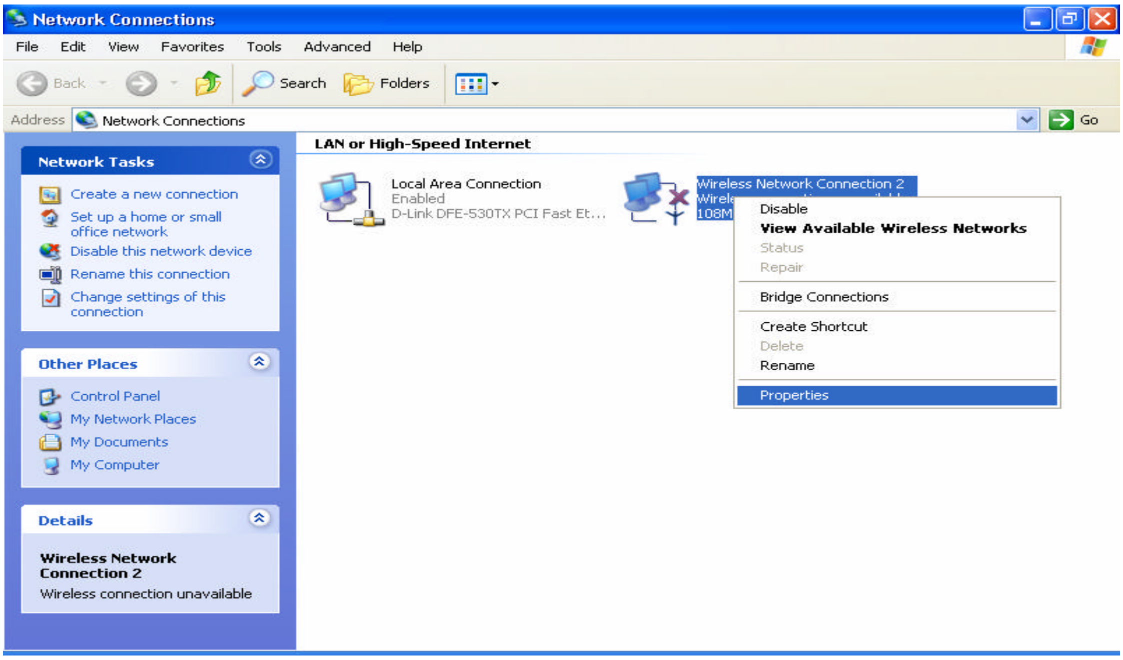
RADIUS Server 2 (Optional)
IP 0.0.0.0
Port 0
Shared Secret

Step 3: Connection as WPA

1. Here we will use Windows XP Wireless Zero Configuration Utility to be the sample connection

Note: The setting page might a bit different in different Windows XP version.

2. Right click "My Network Place" on your desktop and click "Properties" (or go to "Start/ Settings/ Network" or double click a network icon which represents your wireless network on system tray where right down your screen).
3. Select your Wireless LAN Card right clicks and selects "Properties".



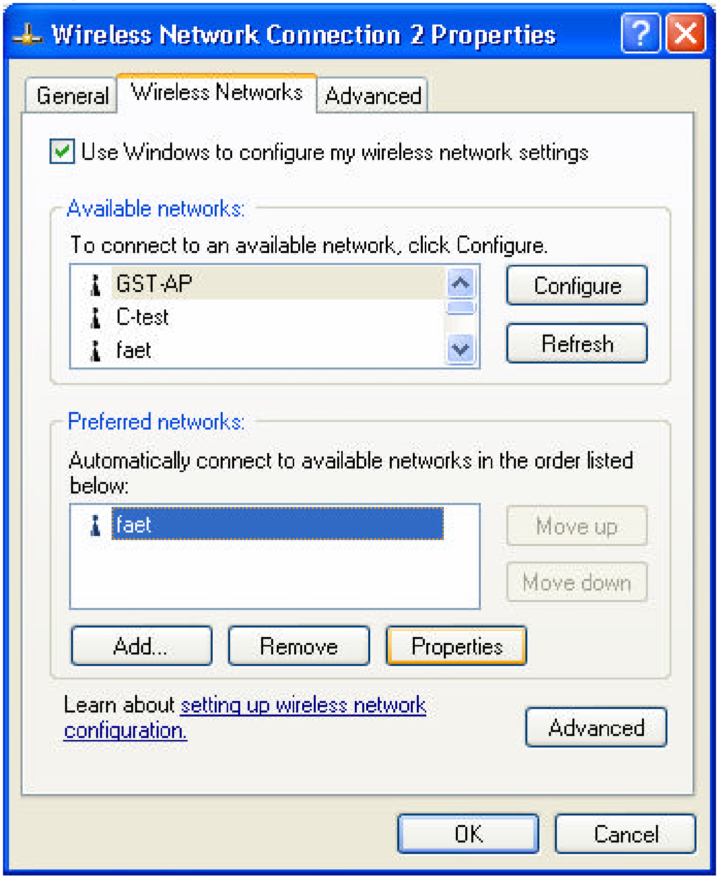
Local Area Connection
Enabled
D-Link DFE-530TX PCI Fast Et...

Wireless Network Connection 2

Wireless Network Connection 2
Wireless connection unavailable

4. Click “Wireless Network”.

5. Select the Access Point which you going to connect and click “Configuration” on its right.



☑ Use Windows to configure my wireless network settings

To connect to an available network, click Configure.

GST-AP
C-test
faet

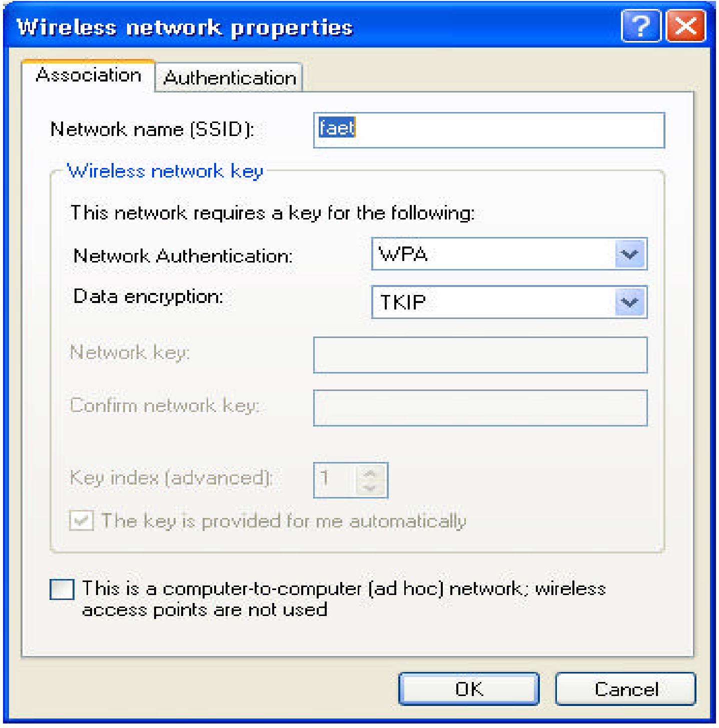
Automatically connect to available networks in the order listed below:

faet

Learn about setting up wireless network configuration.

4. Select "WPA" on Network Connection, and use "TKIP" for Data Encryption.

Note: Currently, AES standard is not finalized yea. if your Access Point and station do support AES you can select AES also.



Wireless network properties

Association | Authentication

Network name (SSID): faet

Wireless network key

This network requires a key for the following:

Network Authentication: WPA

Data encryption: TKIP

Network key:

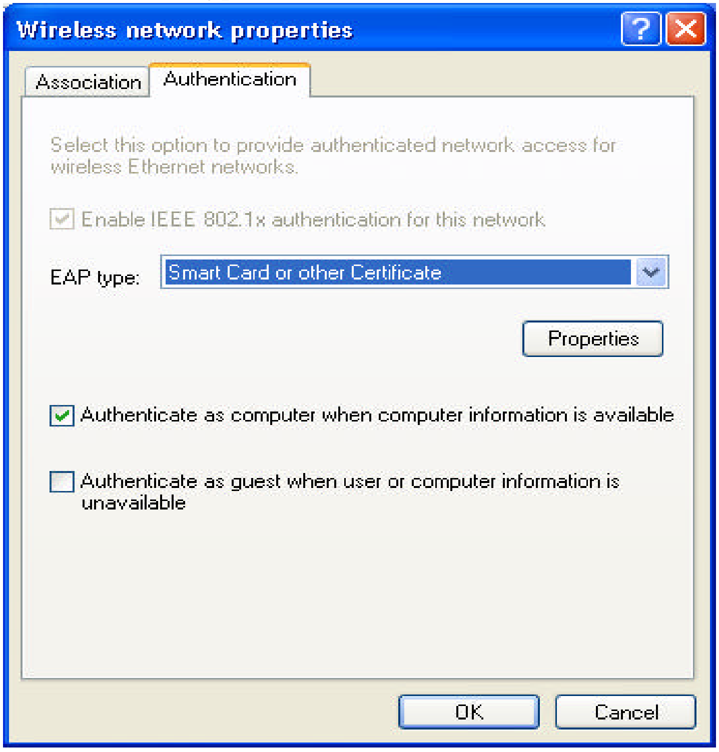
Confirm network key:

Key index (advanced): 1

☑ The key is provided for me automatically

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

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



Wireless network properties

Association | Authentication

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

☑ Enable IEEE 802.1x authentication for this network

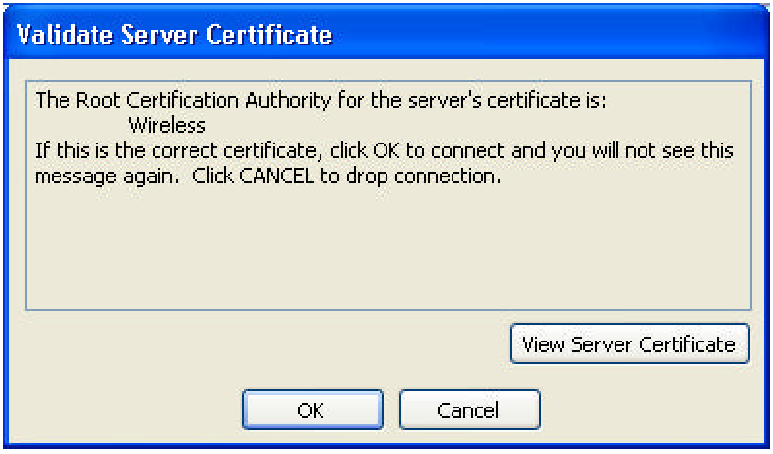
EAP type: Smart Card or other Certificate

☑ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

6. When Station connected to AP, a connection process request will right your screen. Click it you can see a pop window as below (If there has more than a CA on your system you will see a CA selection screen first)

Note: New Windows version can handle it automatically, you might see the latest step directly.



Validate Server Certificate

The Root Certification Authority for the server's certificate is:
Wireless
If this is the correct certificate, click OK to connect and you will not see this message again. Click CANCEL to drop connection.