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 charcters128 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.



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.

D D-Link AirPlus			
Link Info Configuration >>>	SSID	default	
Encryption	Wireless Mode Channel	Infrastructure	4x Config 4x Disable
<u>SiteSurvey</u> About	TxRate	Auto	(• 4x Enable
	Preamble	Long Preamble	
	Power Mode	Continuous Access Mode 💌	
	1	Apply Car	ncel

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 Prop	erties 🛛 💽 🔀			
Network name (SSID):	faet			
Wireless network key (WEP)				
This network requires a ke	ey for the following:			
🔽 Data encryption (WB	P enabled)			
Network Authentical	tion (Shared mode)			
Network key:	ааааа			
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-cor access points are not use	nputer (ad hoc) network; wireless ed OK Cancel			

Part 2: WPA-PSK

Since WPA-PSK standard is an extention 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.

works for People		High-Spe	Air	Plus TREME Wireless A	G ccess Poin
	Home	Advanced	Tools	Status	Help
	Ch: Authentic	annel : 6 💌 ation : C Open Sy Passphrase : 🕬	stem C Shar	red Key C WPA	• WPA-PSK
	Confirm	ed Passphrase : www	iololok	~	0
				Арр	ly Cancel He

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 proper	ties 🛛 🕐 🔀
Association Authentication	
Network name (SSID): Wireless network key This network requires a ke	faet
Network Authentication:	WPA-PSK
Data encryption:	TKIP
Network key:	•••••
Confirm network key:	•••••
Key index (advanced):	1 💭 me automatically
This is a computer-to-con access points are not use	nputer (ad hoc) network; wireless
	OK Cancel

Part 3: 802.1x and WPA

Part 3-1: RADIUS Server Installation

WPA implementation requires RADUIS 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".

Windows Components You can add or remove compo	nents of Windows 2	2000.
To add or remove a componen part of the component will be in Details.	t, click the checkbo stalled. To see wha	x. A shaded box means that only at's included in a component, click
Components:		
Cluster Service		2.5 MB 🔺
🗹 📴 Certificate Services		1.4 MB
🗹 🗭 Indexing Service		0.0 MB
🔽 😭 Internet Information Services (IIS)		21.7 MB 🗾
Description: Includes Window	s Accessories and l	Jtilities for your computer.
Total disk space required:	2.1 MB	Details
	1186.2 MB	Details
Space available on disk:		

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

Windows Components Wizard	×
Certification Authority Type There are four types of certification authorities.	
Certification Authority types:	Description:
 Enterprise root CA 	The most trusted CA in an
C Enterprise subordinate CA	before Divorter CA. Requires
Stand-alone root CA	Active Directory.
C Stand-alone subordinate CA	<u>_</u>
Advanced options	
	< Back Next > Cancel

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

Windows Components Wizard		×
CA Identifying Information Enter information to identify t	this CA	1
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 Pt	
	< Back Next > Cano	el

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.

🙀 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 Bequest

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

6. Right Click on your Domain and click "Properties".

dive Directory Users and Compute	rs		_ 🗆 🗙	
] 🥪 ⊆onsole Window Help			_ 8 ×	
_ Action View ← → 🗈 📧 😭 🚱 😫 🦉 🖉 🦢 🖓 🍕 📁				
Tree faet.local 5 ob	jects			
Active Directory Users Active Directory Users Control Connect to Domain Connect to Domain Controller Coperations Masters New All Tasks View	Type builtinDomain Container Organizational Container Container	Description Default container for upgr Default container for new Default container for secu Default container for upgr		
New Window from Here Refresh Export List	_			
Properties				
Opens p Help				

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

faet.local Properties		<u>? ×</u>	
General Managed By Group Policy			
Current Group Policy Object Links for	r faet		
Group Policy Object Links	No Override	Disabled	
🚅 Default Domain Policy			
Group Policy Objects higher in the list have the h This list obtained from: fae34.faet.local	ighest priority.		
New Add Edit		Up	
Options Delete Properties		Down	
Block Policy inheritance			
OK	Cancel	Apply	

8. Select Computer configuration > Security Setting > Public Key Policies9. 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.

🚮 Group Policy		
] Action ⊻iew] ← → 🔁 [• • •	
Tree	Automatic Certificate Request 🗠	
Default Domain Policy [fae34.fae Computer Configuration Gorden Software Settings Windows Settings Windows Settings Gorden Software Setti		
Truste New	Automatic Certificate Request	
⊕	sh t List	
Create a new Automatic Certificace Requ	rest object and add it to the Security Configu	<u>></u>

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

Automatic Certificate Request Setup Certificate Template The next time a computer logs on, a provided.	Wizard
A certificate template is a set of pred computers. Select a template from th Certificate templates:	lefined properties for certificates issued to the following list.
Name Computer Domain Controller Enrollment Agent (Computer) IPSEC	Intended Purposes Client Authentication, Server Authentication Client Authentication, Server Authentication Certificate Request Agent 1.3.6.1.5.5.8.2.2
•	>
	< Back Next > Cancel

- 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.



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"

lows components wizaru			
₩indows Components You can add or remove comp	oonents of Windov	vs 2000.	
To add or remove a compone	ent, click the chec	(box. A shaded boy	means that only
Details.			
Components:			
🗹 😋 Internet Information S	ervices (IIS)		21.7 MB 🔺
🗆 貴 Management and Mo	nitoring Tools		5.2 MB
🔲 🚾 Message Queuing Services			2.6 MB 🛁
🗹 🛃 Networking Services	🗹 🚽 Networking Services		
□ ♣ Other Network File and Print Services			0.0 MB 🚬
Description: Contains a varie	ty of specialized, i	etwork-related servi	ices and protocols.
Total disk space required:	0.4 MB		Dataila
Space available on disk:	1169.9 MB		Details

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				
🗆 畏 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 accoun users. IAS supports the RADIUS protocol.	ting of dial-up and VPN				
Total disk space required: 0.4 MB	Details				
Space available on disk: 1169.3 MB					
0	K Cancel				

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

🐤 Internet Au	uthentication S	ervice				
Action View						
Tree			Friendly Name	Address	Protocol	
P Internet Aut	hentication Servi Open New Client New View Export List Help	ce (Local)	1			

- 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.

lient address (IP or DNS):	:			
192.168.1.1				Verify
lient-Vendor:				
RADIUS Standard				-
Client must always sen	d the signature	attribute in the re	quest	
hared secret:	инин			
Confirm shared secret:	****			

9. Right click on "Remote Access Policy" and select "New Remote Access Policy"

🐤 Internet Authentication Service		
$]$ Action View $] \Leftrightarrow \Rightarrow]$ \blacksquare \blacksquare \blacksquare		
Tree	Name	Order
Internet Authentication Service (Local) Clients Remote Access Logging Remote Access Patients Open New Remote Access Policy New View View Export List Help	Allow access if dial-in permission is enabled	1
Exports the current list to a file		

- Type a name for new policy, press "Next".
 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			
•				
<u></u>				
	Add Cancel			

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



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

? X

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;
Add Remove Edit
If a user matches the conditions
 Grant remote access permission
C Deny remote access permission
Access will be granted with the profile you specify, unless access is overridden on a per-user basis.
Edit Profile
OK Cancel Apply

15. Select Authentication method: tick "Extensible Authenticatio n 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.

Edit Dial-in Profile			<u>? ×</u>				
Dial-in Constraints	IP	М	fultilink				
Authentication	Encryption	Adv	vanced				
Check the authentication meth	Check the authentication methods which are allowed for this connection.						
Extensible Authentication	n Protocol						
Select the EAP type which is	acceptable for th	nis policy.					
Smart Card or other Certifica	ate	▼ Config	gure				
Microsoft Encrypted Aut	nentication version	n 2 (MS-CHAP v	v2)				
Microsoft Encrypted Auth	nentication (MS-C	HAP)					
Encrypted Authentication	Encrypted Authentication (CHAP)						
Unencrypted Authentica	Unencrypted Authentication (PAP, SPAP)						
Unauthenticated Access-							
Allow remote PPP clients any authentication metho	to connect witho od.	out negotiating					
	ОК	Cancel	Apply				

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

🥦 Internet Authentication Service			
Action View ← → 🛍 🖬 🗙 😭 🗔	[⊉] + ◆		
Tree	Name		Order
Internet Authentication Service (Local) Clients Remote Access Logging Remote Access Policies	MD5		2
,			

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

Active Directory User	rs and Computers					
		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	1 Non 1977 1 Non 1 No	الت التلكر		
<u>] Accion Mew</u>  ] <⊐ .			12 124 100 V % 12			
Tree	Users 21 objects	1				
ntive Directory Users	Name	Туре	escription			
🖻 🔂 faet.local	Administrator	User	uilt-in account for admini			
🕀 📃 Builtin	Cert Publishers	Security Group	interprise certification an			
Computers	DHCP Adminis	Security Group	lembers who have admini			
E Correign Security	CONCEPTION OF CONCEPTION	Security Group	lembers who have view			
		Security Group	NS Administrators Group			
0.000	Subsupdaterr	Security Group	ins clients who are permi			
	Domain Admins	Security Group	lesignated administrators			
	Domain Comp	Security Group	workstations and serve			
	Domain Cuests	Security Group	Il domain condrollers in ch			
	Domain Lisers	Security Group	ll domain yaests			
	TEnterprise Ad	Security Group	uoman users Isionated administrators			
	Group Policy	Security Group	Tembers in this group can			
	Guest	User	uilt-in account for quest			
	IUSR FAE34	User	uilt-in account for anony			
	IWAM FAE34	User	uilt-in account for Intern			
	👧 krbtat	User	ey Distribution Center Se			
	RAS and IAS	Security Group	ervers in this group can			
	Schema Admins	Security Group	Designated administrators			
	🕵 TsInternetUser	User	his user account is used			
	🕵 kent	User				
			Copy			
			Add members to a group			
			Disable Account			
			Reset Password			
			Open home page			
			Send mail			
			Delete			
			Rename			
			Refresh			
			Properties			
	l		Help			

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

kent Propertie <del>s</del>	<u>? ×</u>
Remote control General Address Account Profile Member Of Dial-in E	Terminal Services Profile   Telephones   Organization   nvironment   Sessions
Remote Access Permission (Dial-in or VP Allow access Deny access	N)
Control access through Hemote Acces     Verify Caller-ID:     Callback Options     No Callback     O Set by Caller (Routing and Remote Access)	ccess Service only)
Always Callback to:     Assign a Static IP Address	· · ·
Define routes to enable for this Dial-in connection.	Static Routes
 ОК	Cancel Apply

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

Edit Dial-in Profile		<u>?</u> ×			
Dial-in Constraints Authentication	IP   Encryption	Multilink Advanced			
Check the authentication	methods which are allo ation Protocol	wed for this connection.			
Smart Card or other Cer	tificate	Configure			
<ul> <li>Microsoft Encrypted</li> <li>Microsoft Encrypted</li> </ul>	Authentication version Authentication (MS-CH	2 (MS-CHAP v2) IAP)			
Encrypted Authentic Unencrypted Auther	<ul> <li>Encrypted Authentication (CHAP)</li> <li>Unencrypted Authentication (PAP, SPAP)</li> </ul>				
Unauthenticated Access	s ients to connect withou iethod.	ıt negotiating			
	ОК	Cancel Apply			

## 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).

Connect to 19	2.168.1.10	? 🛛
		K
Connecting to 19	2.168.1.10	
<u>U</u> ser name:	🕵 kent	×
Password:	••••	
	Remember my password	
	ОК	Cancel

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



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

🗿 Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	A*
🕞 Back 🔹 🕥 - 💌 🛃 🏠 🔎 Search 🤶 Favorites 🜒 Media 🚱 🖾 - 😓 🧮	
Address 🗃 http://192.168.1.10/certsrv/certrqus.asp	🖌 🄁 Go 🛛 Links 🂙
Microsoft Certificate Services Wireless	Home
Choose Request Type	
Please select the type of request you would like to make:	
<ul> <li>User certificate request:</li> </ul>	
<ul> <li>Advanced request</li> </ul>	
	Next >
	~
Done	🥏 Internet

- 6. User Certificate Identifying Information, press "Submit".7. CA warning message will pop up, press "Yes".

Potentia	al Scripting Violation	
1	This Web site is requesting a new trusted Web sites to request a c Do you want to request a certifi	v certificate on your behalf. You should allow only ertificate for you. ate now?

8. Click "Install this certificate"



9. Confirm adding this CA, press "Yes".

Root Cei	rtificate Store	×
1	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, 200 Serial Number : 47AED71F FD477EBD 40FAAD0E 846EAF3D Thumbprint (sha1) : C9921D92 D32C4481 552D90EC 548DE689 8D786B10 Thumbprint (md5) : 71723801 EDA22805 6FF11782 614DB755 Yes No	05

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.

1	High-Spe	ed 2.4GHz V	Vireless A	ccess F
Home	Advanced	Tools	Status	Hel
802.1X				
Encryption Key RADIUS Server 1	Length © 64 Lifetime 30 Min IP Port	bits C 128 bits nutes 192.168.0.10 1812		
RADIUS Server 2 (Optional)	IP Port Shared Secret	0.0.0		

#### 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"

🕹 Wireless Network Connectio	on 2 Properties 👘 ? 🔀
General Wireless Networks Advar	nced
Use Windows to configure my w Available networks: To connect to an available netwo	ireless network settings rk, click Configure.
& GST-AP	
L C-test	Refresh
Automatically connect to available below:	e networks in the order listed
	Move down
Add Remove	Properties
Learn about <u>setting up wireless ne</u> <u>configuration.</u>	twork Advanced
	OK Cancel

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

faet properties	? 🛛
Association Authentication	
Network name (SSID): Wireless network key This network requires a k	faet
Network Authentication:	Open 🔽
Data encryption:	WEP 🔽
Network key:	
Confirm network key:	
Key index (advanced):	1 Contraction of the second se
This is a computer-to-co access points are not u	omputer (ad hoc) network; wireless sed
	OK Cancel

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

faet proper	ties	?	×
Association	Authentication		_
Select this wireless Eth	option to provide authentic iernet networks.	ated network access for	
🗹 Enable	EEE 802.1x authenticatio	n for this network	
EAP type:	Smart Card or other Certi	ficate 💊	-
V Authent Authent	cate as computer when c cate as guest when user ( ble	omputer information is availab or computer information is	ble
		OK Cance	

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).

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.
View Server Certificate OK Cancel

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".

D-Link Building Networks for People		High-Spe	Air R	Plus TREME Wireless A	<b>G</b> ^{rm} ccess Point
DWL-2000AP	Home	Advanced	Tools	Status	Help
Wizard Wireless LAN DHCP	Wireless Setti AP N Cha Authentic	ngs Jame : DWL-2000AP SSID : faet annel : 6 ▼ ation : C Open Sy	stem C Shar	ed Key ⓒ WPA V App	C WPA-PSK

- 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.

1		High-Spe	ed 2.4GHz V	Vireless A	Access F
Home	e 🔽	Advanced	Tools	Status	Hel
802.1X					
		Enabled	O Disabled		
Encryption	Key	Length 🖲 64	bits C 128 bits		
		Lifetime 30 Mi	nutes 💌		
RADIUS Se	erver 1	IP	192.168.0.10		
		Port	1812		
		Shared Secret	skokokok		
RADIUS Se	erver 2	IP	0.0.0.0		
(Optional)		Port	0		
		Shared Secret			

### 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"

- Wireless Network Connection 2 Prope	rties 🛛 ? 🔀
General Wireless Networks Advanced	
Vindows to configure my wireless network	k settings
I o connect to an available network, click Lonfi	gure.
L C-test	coningure
🖌 faet 🔍	Refresh
Automatically connect to available networks in t below:	he order listed
	Move down
Add Remove Properties	
Learn about <u>setting up wireless network</u> configuration.	Advanced
ОК	Cancel

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

Wireless network propertie	98	? 🛛
Association Authentication		
Network name (SSID):	et	
This network requires a key f	or the following:	
Data encryption:	TKIP	*
Network key:		
Confirm network key:		
Key index (advanced): 1	automatically	
This is a computer-to-compu access points are not used	iter (ad hoc) network; wii	reless
	ОК	Cancel

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.

Validate Servei	Certificate
The Root Certific Wireles If this is the corre message again.	ation Authority for the server's certificate is: s act certificate, click OK to connect and you will not see this Click CANCEL to drop connection.
	View Server Certificate OK Cancel

~ End of Document ~