

D-Link DRS-200

Ethernet Authentication

Radius Server

Manual

D-Link

Building Networks for People

10272003

Contents

Package Contents.....	2
Introduction.....	3
Getting Start.....	11
Using the Network Configuration.....	13
Setup Authentication in client.....	39
Connecting Additional Computers To The DRS-200.....	60
Resetting the DRS-200 to the Factory Default Settings.....	62
Contacting Technical Support.....	63
Warranty and Registration.....	64

Package Contents



Contents of Package:

- D-link DRS-200 Radius Server
- Power Adapter – 5V DC
- Ethernet (CAT5-UTP/Straight-Through) Cable
- Manual on CD
- Quick Installation Guide

Note: Using a power supply with a different voltage rating than the one included with the DRS-200 will cause damage and void the warranty for this product.

If any of the above items are missing, please contact your reseller.

System Requirements For Configuration:

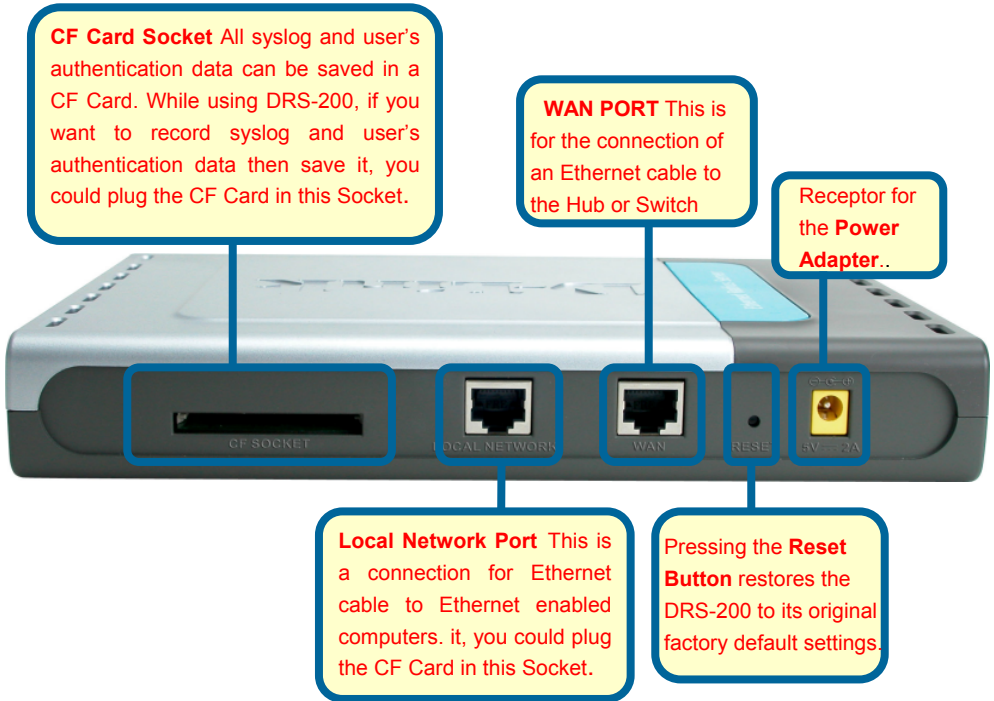
- Ethernet-Based Cable or DSL Modem
- Computer with Windows, Macintosh, or Linux-based operating system with an installed Ethernet adapter
- Internet Explorer version 6.x or Netscape Navigator version 6.x and above, with JavaScript enabled

Introduction

Wireless networking is not only considered to be a mobile or convenience but also is seen as an integral tool for business success today. Here comes the potential for unauthorized access, eavesdropping or other security issues. For enhancing security of your wireless network, DRS-200's user identification, data authentication and other applications seem to be the most practical and effective solutions now.

By the deployment of IEEE 802.1.X protocol and Radius Server- DRS-200, any wireless network accessing could be controlled safely. Before accessing IEEE 802.1.X wireless network environment, users have to get user names, passwords and Digital Certificate through EAPOL (Extensible Authentication Protocol Over LAN) and Access Point. And then they could go further to be authorized by Radius Server and access Internet with legal identities.

Connections



*Note: System log and Radius log won't be saved if you don't have CF card in your DRS-200, and all these log files will be lost after power off. An 8MB CF card could be used to save at about 200 thousand records of log data in average. (This number may vary depends on the length of each record) and 100 records each of client data and user's authentication data. The **DRS-200** has the following CF card as described below:*

CF card capacity	Client data entry	User's authentication data entry	System log and Radius log data entry
8MB	100	100	200 thousand
16MB	100	100	400 thousand
32MB	100	100	800 thousand

Features & Benefits

■ **Secure Network**

Unauthorized users, illegitimate access, data interception and other perceived concern of wireless network security have obviously countervailed the power of WLAN popularization. For privacy over airwave, besides helping you to deploy more intelligent user-authentication, the data-encryption provided by DRS-200 could be the second line of defense to prevent any breaking against your internal network.

■ **Security Authentication**

DRS-200 provides "MD5-Challenge", "Transport Level Security (TLS)" and "MAC Authentication" three authentication methods based on EAP for negotiation between the remote access client and the authenticator. MD5 is to authenticate the credentials of remote access clients by using user name and password security systems, TLS is designed to provide secure authentication and encryption for a TCP/IP connection, and MAC authentication provides a means of authenticating without the user login required by the web-based and 802.1X methods.

■ **Supports 802.11X draft standard**

DRS-200 supports WLAN within multiple 802.11X draft standards such as 802.11a, 802.11b and 802.11g. Well-known 802.11b standard operating in 2.4 GHz bandwidth and supports a maximum data rate of 11Mbps has served almost the entire WLAN market today. The follow-up standard 802.11a (5GHz/ 54Mbps) and 802.11g (2.4GHz/ 54Mbps) which compatible with 802.11b substantially raised data rate, serve range for future market demand.

Features & Benefits continued

■ **Compatibility with well-known providers' AP**

DRS-200 is compatible with most of Access Points (AP) from well-known providers such as Cisco, D-Link, Avaya, Orinoco and etc. It also provides the quota of 100 authentications for users accessing Internet through AP. And specifications of the above will give you more convenience for DRS-200 deployment.

■ **Instant installation without concern about OS**

Windows XP and Windows Server 2003 have built-in support for Wi-Fi (IEEE 802.11b) wireless access and IEEE 802.1X authentication using the "Extensible Authentication Protocol" (EAP). Windows 2000 supports IEEE 802.1X authentication when "Microsoft 802.1X Authentication Client" is installed. So you just need making sure the physical connection of wireless environment is well and to configure "Radius setup" for DRS-200 proceeding further user authentication.

■ **WEB user interface environment**

By accessible, simple operating interface, you can use DRS-200 without any complicated steps or high-tone, professional MIS (Management Information Service) knowledge. Besides, DRS-200 can be configured and upgraded firmware on site or anywhere on Internet.

■ **Data save in the CF Card**

DRS-200 can save system log (Administrator logon, setup or modifying DRS-200 system records) and authentication log (User has been authenticated records by DRS-200) in the CF Card. In the future, it can include other relevant information.

Introduction to WLAN

Wireless local area networks (wireless LANs, or WLANs) uses wireless transmissions, such as radio or infrared instead of phone lines or fiber-optic cable to connect data devices. That means the use of mobile computing devices, such as laptops and personal digital assistants, coupled with the demand for continual network connections without “plug in,” are driving the adoption of enterprise WLANs. Network managers are using WLANs to facilitate network moves, adds and changes. In addition, the inherent flexibility of WLANs overcomes limitations created by older buildings, leased spaces, or temporary work areas.

Introduction to RADIUS

RADIUS (Remote Authentication Dial-In User Service) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. RADIUS now supports virtual private network (VPN) servers, wireless access points, authenticating Ethernet switches, Digital Subscriber Line (DSL) access, and other network access types.

Introduction to IEEE 802.1x

The IEEE 802.1X standard for Port-based authentication is a layer 2 solution between client and wireless access point or switch. In the 802.1X framework authentication information is carried using the Extensible Authentication Protocol (EAP, RFC 2284), a protocol that enables the use of several authentication methods, currently MD5, TLS, TTLS, MS-CHAPv2, PEAP and SIM-card based.

802.11 Wi-Fi is the state of the art WLAN today. 802.11 has two physical layer standards: 802.11b operating at 2.4GHz (and delivering up to 11Mbps at 250 feet max) and 802.11a operating at 5GHz (and delivering up to 54Mbps at 150 feet max). A third standard, 802.11g, providing the speeds of 802.11a at the distances of 802.11b, should be finalized in late 2003. Although most WLANs today are 802.11b, most enterprises will use 802.11a

Introduction to EAP-TLS

EAP-TLS is based on SSL v3.0. To better understand EAP-TLS operation, this section focuses on the operation of TLS with respect to SSL. TLS is designed to provide secure authentication and encryption for a TCP/IP connection.

Introduction to EAP-MD5 CHAP

EAP-Message Digest 5 Challenge Handshake Authentication Protocol (EAP-MD5 CHAP) is a required EAP type that uses the same challenge handshake protocol as PPP-based CHAP, but the challenges and responses are sent as EAP messages. EAP-MD5 CHAP is described in RFC 2284.

A typical use for EAP-MD5 CHAP is to authenticate the credentials of remote access clients by using user name and password security systems. You can also use EAP-MD5 CHAP to test EAP interoperability.

Introduction to MAC Authentication

On the RADIUS server, instead of entering user names, you enter the MAC addresses, which are allowed to authenticate. Then, when a MAC address attempts to access a port, the device sends the MAC authentication password and the MAC address to the RADIUS server for authentication. Automatic re-authentication is available with MAC authentication.

Introduction to Bridge

In telecommunication networks, a bridge is a product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, Ethernet or Token Ring). A bridge examines each message on a LAN, "passing" those known to be within the same LAN, and forwarding those known to be on the other interconnected LAN (or LANs).

LEDS

LED stands for **L**ight-**E**mitting **D**iode. The **DRS-200** has the following LEDs as described below:



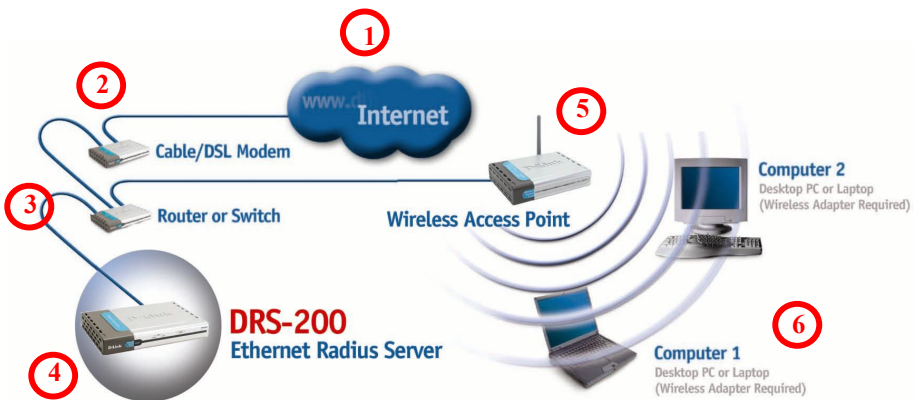
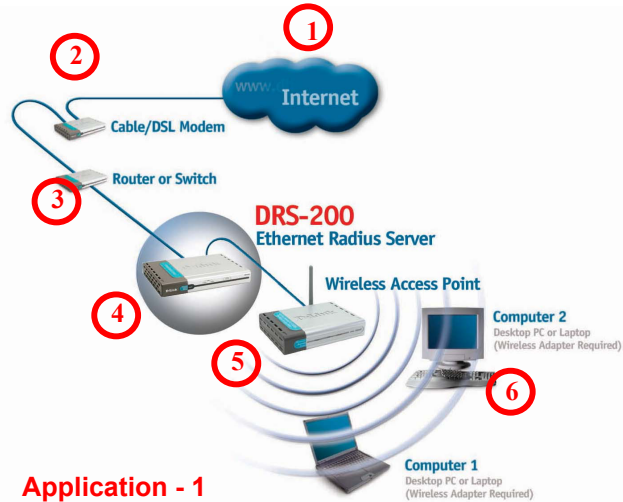
LED		LED Activity	
Power	Green	Power ON	
WLAN	Link Indicator	ON	On line
		OFF	Off line
	Active Indicator	Sparkling Data transmission	
Local Network	Link Indicator	ON	On line
		OFF	Off line
	Active Indicator	Sparkling Data transmission	

Getting Started

With its default settings, the DRS-200, when activated, will connect with other D-Link Express Wireless network products, right out of the box.

Please refer to the following sections of this manual for additional information about setting up a network:

Setup Authentication in client—learn how to setup authentication in client, then can connection Wireless Access Point to Internet
Using the Configuration Menu - learn the settings for the DRS-200, using the web-based interface.



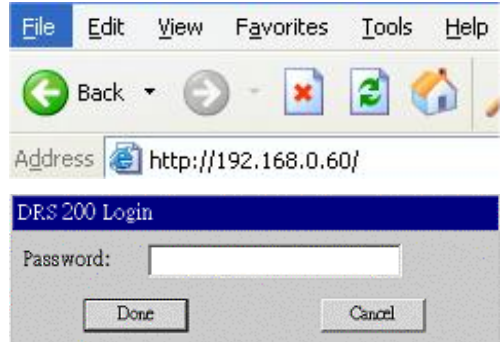
For a typical network setup at home/office (as shown above), please do the following:

- 1** You will need broadband Internet access (a Cable or DSL subscription line into your home or office)
- 2** Consult with your Cable or DSL provider for proper installation of the modem
- 3** You can use Hub or Switch(e.g.,**LINK DFE-2624ix**) to connection Wireless Access Point and DRS-200.
- 4** Connect the Hub or Switch to the DRS-200 Wan Port (See the Quick Installation Guide included with the DRS-200.)
- 5** Connect the Hub or Switch to the Wireless Access Point(e.g.,**DWL-900AP+**)
- 6** If you are connecting a laptop computer to your network, install the drivers for the Card bus adapter (e.g., **D-Link DWL-650+**) into a laptop computer

Using the Network Configuration

For using further applications of DRS-200, you have to set up related configurations by following steps after reboot the PC.

- Open the PC Web browser. (Ex: Microsoft Internet Explorer)
- Enter "**192.168.0.60**" in the Address or Location box.
- Click the "**DONE**" button.



Note: If you have changed the default IP

Address assigned to the DRS-200, make sure to enter the correct IP Address.

When entering the WEB management interface of DRS-200, you'll find the following main items on the screen.



◆ **Basic Setup**

Includes "Primary Setup" and "Radius Setup" configuration.

◆ **Advance Setup**

Includes SNMP and export/import system configuration.

◆ **Network Info**

This item shows system and radius status, you can setup password here too.

◆ Help

If you have any problem while operating or configuring, please click this button to request more online user guide.

◆ Save Data & Logout

There're 3 tabs on the right below of the main page. You could use these buttons to save data, to logout DRS-200's configuration or to request Online Help.

Using the Network Configuration



Save

When you changed configurations in each item, you have to use "Save" button to save new configurations



Exit

After saving and activating DRS-200, you can click the "Logout" button or close the window to leave the DRS-200 management interface.

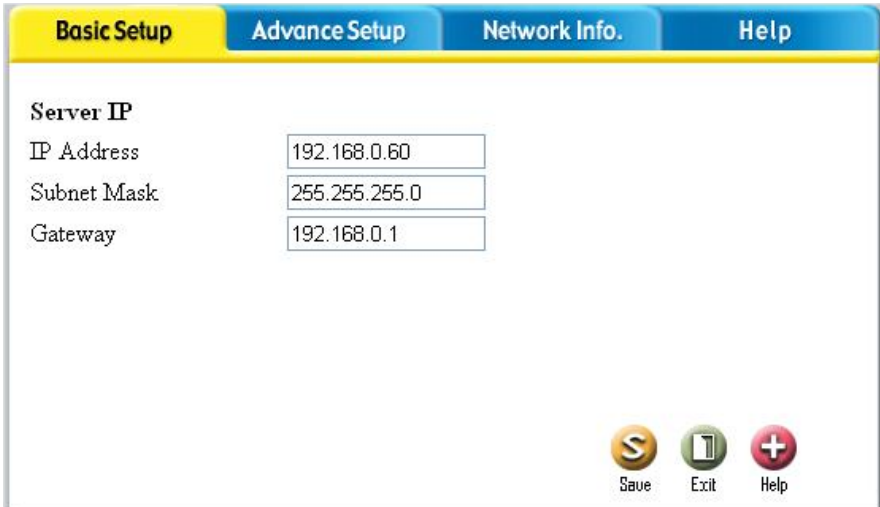


Help

If you have any problem while operating or configuring, please click this button to request more online user guide.

Using the Network Configuration

Basic Setup > Primary Setup



Server IP	
IP Address	192.168.0.60
Subnet Mask	255.255.255.0
Gateway	192.168.0.1

Save Exit Help

When you click the " Primary Setup" tab, you'll see the " Basic Setup " menu. This item can let you set up the different IP Address and Subnet Mask of DRS-200 in your internal network/LAN, and makes DRS-200 a Gateway for other PCs connecting to the Internet.

IP Address- There's a default IP "196.168.0.60" in the "IP Address" column. You can enter an unused IP Address within the range used by one segment of your LAN. It will be the LAN IP of DRS 200. Please click "Save" button after you entered a new IP. At the same time, you have to change the Class C of your administrator's PC IP as same as DRS-200.

Subnet Mask- For example, the value "255.255.255.0" is standard for small (class "C") network. For other network, use the Subnet Mask for the LAN segment to which the DRS-200 is attached (the same value as the PCs on that LAN segment).

Gateway- Please enter the Gateway IP you have already setup.

NOTE : After you entered above essential data in this page/item, you have to click the "Save" button on right below of the screen.

Using the Network Configuration

Basic Setup > Radius Setup

Basic Setup **Advance Setup** **Network Info.** **Help**

RADIUS Setup

Server Configuration

Private Key Password

Private Key File

Certificate File

CA File

Client Configuration

IP Address

Secret

Shortname

Client List

Index	IP Address	Secret	Shortname	Configure
-------	------------	--------	-----------	-----------

User Configuration

Select Authentication Type







Authentication Type : MD5

User Name

Password

User List

Index	TYPE	UserName	Password	Configure
-------	------	----------	----------	-----------

Start Restart Stop Save Exit Help

DRS-200 provides three authentication types, "TLS", "MAC" and "MD5". Administrator can enter data of authentication algorithm and setup Wireless Access Point. There're 3 tabs on the right below of the main page. You could use these buttons to choose authentication types.

Using the Network Configuration

How to save data and activate DRS-200' Radius

If you have changed and saved DRS-200's Radius Setup and want DRS-200's Radius be activating, you have to use following three button in the item "Radius Setup" of "Basic Setup".



Start

If you've changed and saved the configuration of Radius, you have to stop the operation of Radius first, then click **"Start"** button to reactivate Radius.



Restart

You can also use **"Restart"** button to reactivate Radius.



Stop

You can also use **"Stop"** button to shot down Radius and then the network will be disconnected. You have to click **"Start"** button to reactivate Radius.

Two processes for activating DRS-200

We recommend the two following procedures for you to activate new configurations and restart system function.

1. Click **"Save"** → Click **"Restart"**
2. Click **"Save"** → Click **"Stop"** → Click **"Start"**

Finally, click **"Exit"** to leave the DRS-200 operating interface.

Using the Network Configuration

Basic Setup > Radius Setup > Server Configuration

The screenshot shows a web interface for RADIUS Setup. At the top, there are four tabs: 'Basic Setup' (highlighted in yellow), 'Advance Setup', 'Network Info.', and 'Help'. Below the tabs is the title 'RADIUS Setup'. The main content is divided into two sections: 'Server Configuration' and 'Client Configuration'. The 'Server Configuration' section contains four rows of input fields: 'Private Key Password' with a 'Save' button; 'Private Key File', 'Certificate File', and 'CA File', each with a 'Browse...' button and an 'Upload' button. The 'Client Configuration' section contains three rows of input fields: 'IP Address', 'Secret', and 'Shortname', followed by 'Add' and 'Reset' buttons. Below this is a 'Client List' table with five columns: 'Index', 'IP Address', 'Secret', 'Shortname', and 'Configure'. The table contains three rows of data, each with a 'Delete' button in the 'Configure' column.

Index	IP Address	Secret	Shortname	Configure
1	192.168.1.1	12312	test1	Delete
2	192.168.1.8	999	test2	Delete
3	192.168.1.19	168	test3	Delete

When administrator uses the TLS type, you can use "Open SSL" to release related data, and upload these data to DRS-200 configuration for authentication.

Private Key Password- Please use the password that was released when you used Open SSL to make authentication files.

Private Key File- Please click “Browse” to open operating window, then choose the file directory where is placed "server_key.pem" which is made by Open SSL. Finally, please click "Upload" to upload the file to DRS-200.

Certificate File- Please click “Browse” to open operating window, then choose the file directory where is placed "server_cert.pem" which is made by Open SSL. Finally, please click "Upload" to upload the file to DRS-200.

Using the Network Configuration

CA File- Please click “Browse” to open operating window, then choose the file directory where is placed " cacert.pem " which is made by Open SSL. Finally, please click "Upload" to upload the file to DRS-200.

NOTE : After you entered above essential data in this page/item, you have to click the "Save" button on right below of the screen.

Using the Network Configuration

Basic Setup > Radius Setup > Client Configuration

Basic Setup **Advance Setup** **Network Info.** **Help**

RADIUS Setup

Server Configuration

Private Key Password

Private Key File

Certificate File

CA File

Client Configuration

IP Address

Secret

Shortname

Client List

Index	IP Address	Secret	Shortname	Configure
1	192.168.1.1	12312	test1	<input type="button" value="Delete"/>
2	192.168.1.8	999	test2	<input type="button" value="Delete"/>
3	192.168.1.19	168	test3	<input type="button" value="Delete"/>

When several Wireless Access Point exist in a network segment, administrators can setup the related information and IP of every Wireless Access Point in this item.

DRS-200 can save up to 100 records of Wireless Access Points data

IP Address- Please enter the IP Address of Wireless Access Point. Please notice that, the IP of Wireless Access Point and DRS-200's IP must exist in the same Class C.

Secret- Please enter the secret value as same as **Wireless Access Point's 802.1X's configuration.**

Short Name- You can define a short name of every Wireless Access Point. This column must not be empty.

After entering data of above three items, please click "ADD" to add in database or click "Reset" to clear data, and fill these columns again.

NOTE : After you entered above essential data in this page/item, you have to click the "Save" button on right below of the screen.

Using the Network Configuration

Basic Setup > Radius Setup > Client List

Basic Setup | **Advance Setup** | **Network Info.** | **Help**

RADIUS Setup

Server Configuration

Private Key Password

Private Key File

Certificate File

CA File

Client Configuration

IP Address

Secret

Shortname

Client List

Index	IP Address	Secret	Shortname	Configure
1	192.168.1.3	1234	AP1	<input type="button" value="Delete"/>
2	192.168.1.20	1234	AP2	<input type="button" value="Delete"/>
3	192.168.1.40	1234	AP3	<input type="button" value="Delete"/>

All settings of Wireless Access Points will show in this "Client List". You can click the "Delete" button to delete existed setting in Configure column.

NOTE : After you entered above essential data in this page/item, you have to click the "Save" button on right below of the screen.

Using the Network Configuration

Basic Setup > Radius Setup > User Configuration

Basic Setup **Advance Setup** **Network Info.** **Help**

User Configuration

Select Authentication Type

Authentication Type : MD5

User Name

Password

User List

Index	TYPE	UserName	Password	Configure
1	MD5	David	1234	<input type="button" value="Delete"/>
2	MD5	Kevin	12567	<input type="button" value="Delete"/>
3	MAC	007788541236	1qaz	<input type="button" value="Delete"/>
4	TLS	Saliy	XXXXXX	<input type="button" value="Delete"/>

In this item, you have three choices of authentication type, these types are MD5, MAC and TLS, and each type can provides the data of authentication users. **DRS-200 can save up to 100 records of user authentication data**

Type- Select

Please click here to choose an authentication type.

Authentication-

Authentication Type- The authentication type you selected will be shown here.

NOTE : After you entered above essential data in this page/item, you have to click the "Save" button on right below of the screen.

Using the Network Configuration

Basic Setup > Radius Setup > User Configuration > MD5

User Configuration

Select Authentication Type

Authentication Type : MD5

User Name

Password

User Name- Administrators can setup user names here.

Password- Please enter the password for USER authentication.

Click "Add" this record in database. You can also click "Reset" to clear User Name, Password, and re-enter again.

NOTE : After you entered above essential data in this page/item, you have to click the "Save" button on right below of the screen.

Using the Network Configuration

Basic Setup > Radius Setup > User Configuration > MAC

User Configuration

Select Authentication Type

Authentication Type : MAC

MAC Address

Password

MAC Address-

Please enter the User's MAC Address. The format must be "XXXXXX-XXXXXX" (12 digits)

Password-

Please enter the "Share Secret" which produced by "AP" authentication.

Click "Add" this record in database. You can also click "Reset" to clear Mac Address, Password, and re-enter again.

NOTE : After you entered above essential data in this page/item, you have to click the "Save" button on right below of the screen.

Using the Network Configuration

Basic Setup > Radius Setup > User Configuration > TLS

User Configuration

Select Authentication Type

Authentication Type : TLS

User Name

User Name-

Administrators can setup user names here. The name must be as same as authentication.

Click "Add" this record in database. You can also click "Reset" to clear user name and, re-enter again.

NOTE : After you entered above essential data in this page/item, you have to click the "Save" button on right below of the screen.

Using the Network Configuration

Basic Setup > Radius Setup > User List

User List

Index	TYPE	UserName	Password	Configure
1	MD5	asd	asdsad	<input type="button" value="Delete"/>
2	MD5	dddd	dddddd	<input type="button" value="Delete"/>
3	TLS	adadddd	XXXXXX	<input type="button" value="Delete"/>
4	MD5	cccccc	zxc	<input type="button" value="Delete"/>
5	TLS	client	XXXXXX	<input type="button" value="Delete"/>
6	MD5	dlink	1234	<input type="button" value="Delete"/>

User List-

User List will show user name and password of every authentication type. (You don't have to setup password in TLS type) . Administrator can delete a user data in Configure by clicking "Delete".

NOTE : After you entered above essential data in this page/item, you have to click the "Save" button on right below of the screen.

Using the Network Configuration

Advance Setup > SNMP

This section is only useful if you have SNMP (Simple Network Management Protocol) software on your PC. If you have SNMP software, you can use a standard MIB II format with the DRS-200.



SNMP

System Information

SNMP Enable Disable



SNMP Enable- Clicking here can activate the SNMP function.

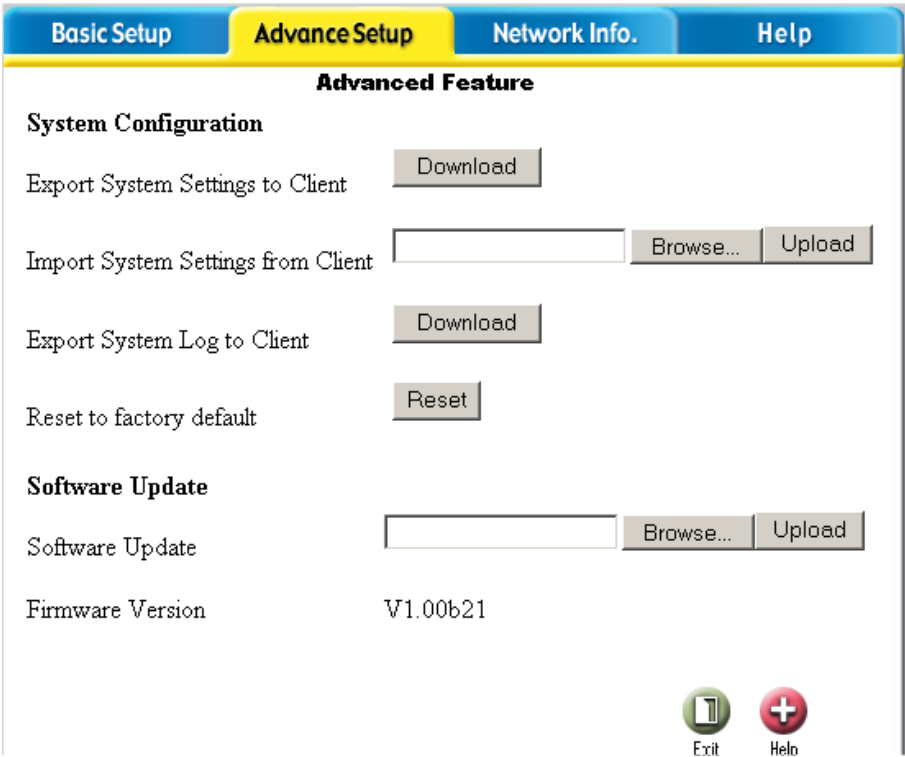
SNMP Disable- Clicking here can close the SNMP function.

NOTE : After you entered above essential data in this page/item, you have to click the "Save" button on right below of the screen.

Using the Network Configuration

Advance Setup > Advanced Feature

This item can let you make a backup of DRS-200 configuration. When any unexpected hardware problem happened, you don't need to set up the configuration again. Besides, you can download the latest updating files or export system log in this item .



Export System Setting to Client-

Please click the "Download" button to download and to save original DRS-200 configuration as a backup.

**Import System
Setting to Client-**

Please click "Browse" button to find your configuration backup file, then click "Upload" button to modify the configuration of DRS-200 automatically.

**Firmware Version-
Software Update-**

This column will show the firmware version of DRS-200. Please click "Browse" button to find the latest updating files you downloaded, then click "Upload" button to upload new software version of DRS-200 automatically.

**Export System Log to
Client-**

Please click on the "Download" button to download DRS-200 System log and Radius Server log and save as plain text format file.

**Reset to factory
default-**

You can click on the "Reset" button if want to DRS-200 configuration reset to factory default value

NOTE : After you entered above essential data in this page/item, you have to click the "Save" button on right below of the screen.

Using the Network Configuration

Network Info. > System Status

System Status	
Server Information	
IP Address	192.168.1.249
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
Device Information	
Loader Version	V 1.00
Firmware Version	V1.0_0917_build2043

Exit Help

IP Address-

It shows the IP address of the DRS-200.

Subnet Mask-

It's the Network Mask (Subnet Mask) for the IP Address above in this column.

Gateway-

The column shows the Gateway IP Address of DRS-200.

Loader Version-

This column shows the version of the Firmware Loader currently installed.

Firmware Version-

This column shows the version of the Firmware currently installed..

*Note: **Loder (Boot Loder)** is the first software program that runs when a device starts. It's responsible for loading and transferring control to the operating system *kernel* software (Like the Linux). **Firmware** is built in Boot Loder to provide other application usage..*

Using the Network Configuration

Network Info. > Radius Setup

Basic Setup Advance Setup **Network Info.** Help



RADIUS Status

Client List

Index	IP Address	Secret	Shortname
1	192.168.0.50	1234	900AP

User List

Index	TYPE	UserName	Password
1	MD5	dlink	1234
2	TLS	client	XXXXXX

 Exit  Help

This item will show all detail of DRS-200's Clients and Users data.

Client List- All settings of Wireless Access Points will show in this "Client List"

User List- User List will show user name and password of every authentication type.

Using the Network Configuration

Network Info. > Admin. Password

Basic Setup	Advance Setup	Network Info.	Help
Admin. Password			
Administrator Password			
Old Password	<input type="password" value="*****"/>	(Enter Old Password)	
New Password	<input type="password" value="*****"/>	(Enter New Password)	
	<input type="password" value="*****"/>	(Re-enter To Confirm)	
   Save Exit Help			

Old Password-

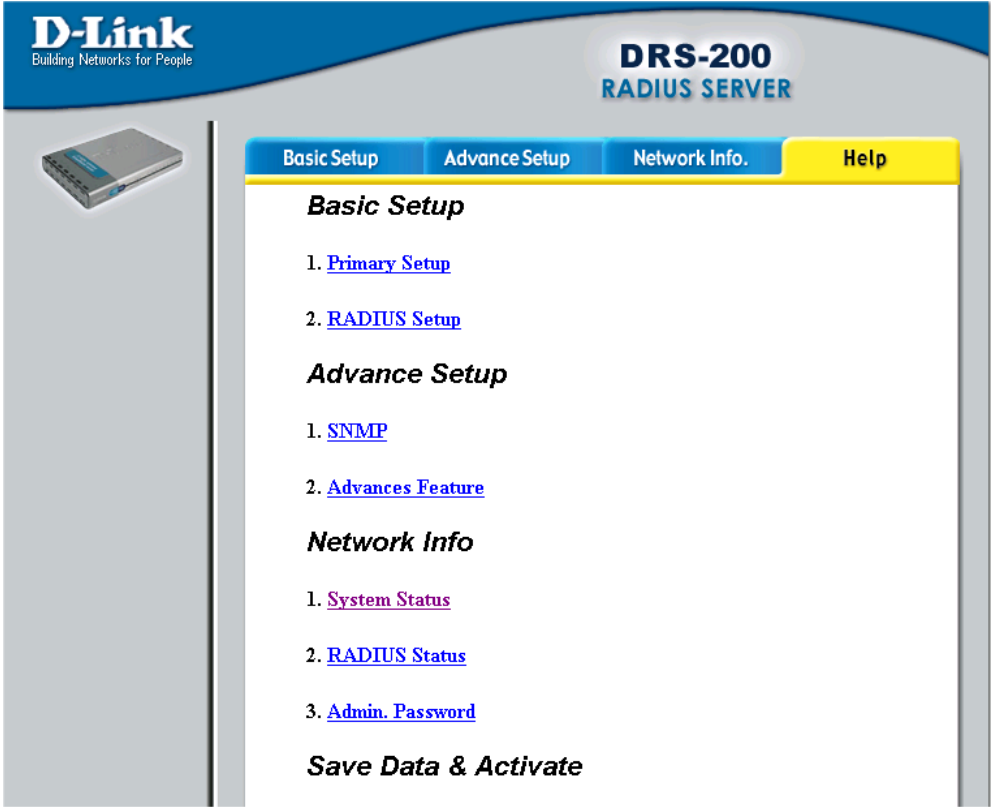
If you want to change the admin password, please enter the password you set before. If you have not ever change the default password, don't need to input the Password in here.

New Password-

After enter the old password in above column, please enter the new password in this column. Then re-enter it again to confirm the password is correct.

NOTE : After you entered above essential data in this page/item, you have to click the "Save" button on right below of the screen.

Using the Network Configuration



D-Link
Building Networks for People

DRS-200
RADIUS SERVER

Basic Setup Advance Setup Network Info. **Help**

Basic Setup

1. [Primary Setup](#)
2. [RADIUS Setup](#)

Advance Setup

1. [SNMP](#)
2. [Advances Feature](#)

Network Info

1. [System Status](#)
2. [RADIUS Status](#)
3. [Admin. Password](#)

Save Data & Activate

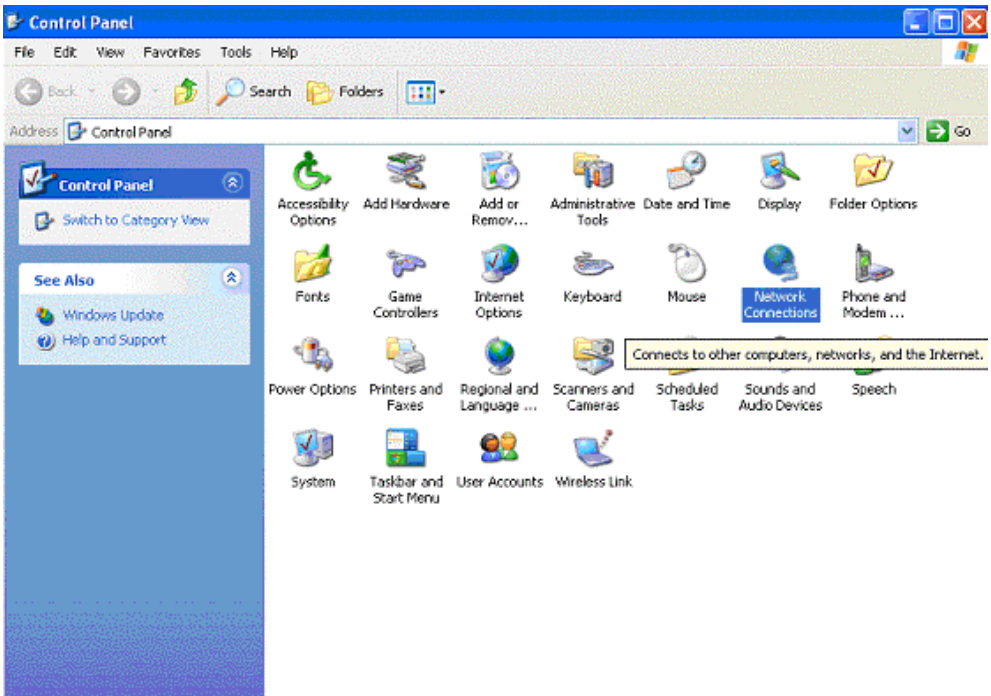
This screen displays the complete **Help** menu. For help at anytime, click the **Help** tab in the Configuration menu.

Setup Authentication in client

Setup MD5 authentication in client

In **Windows XP Operating System**, it's available for **MD5 authentication** in the item "**Control Panel**". You can carry out the certificate by following steps.

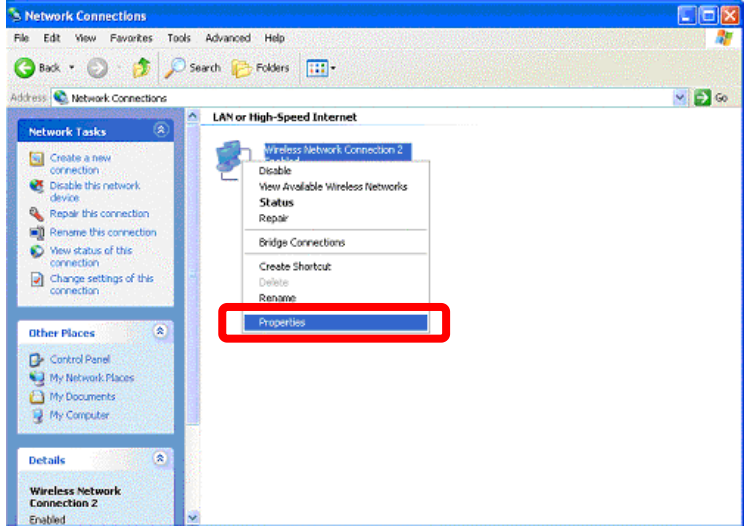
- Go to **Start Click Start (in the lower left corner of the screen)**
- Select **Control Panel** and click
- After open, select **Network Connections** and click



Setup Authentication in client

Setup MD5 authentication in client

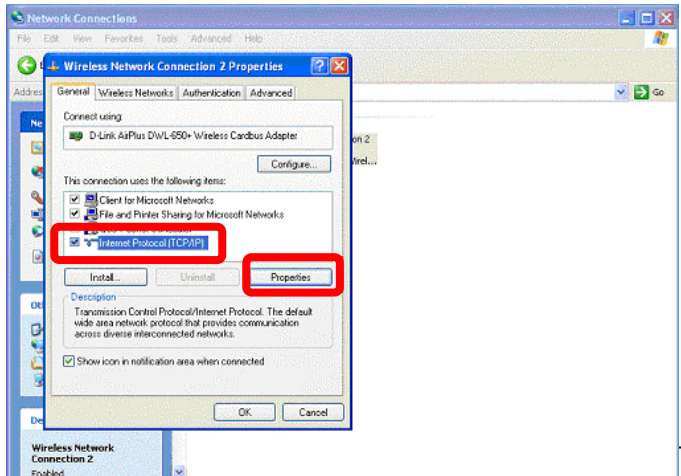
- Select **"Properties"** on **"Wireless Network Connection"** icon.



- When the dialogue window **"Wireless Network Connection Properties"** pops up

- Choose **"Internet Protocol (TCP/IP)"**

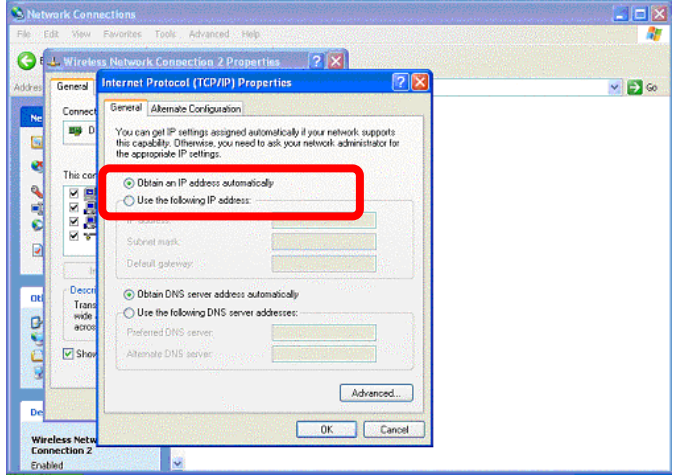
- Click **"Properties"**



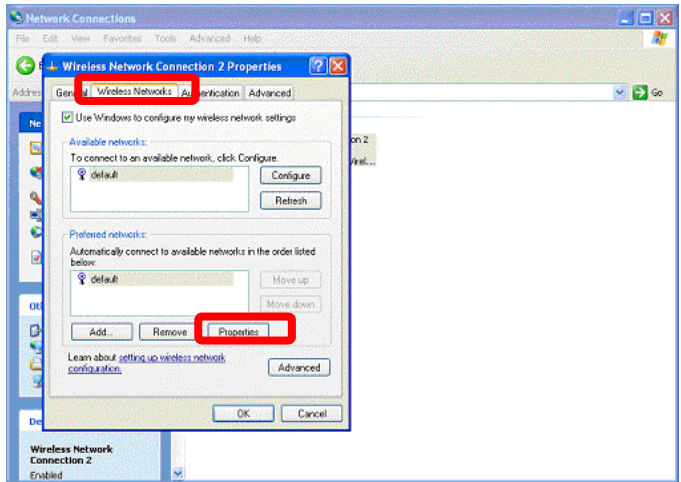
Setup Authentication in client

Setup MD5 authentication in client

- Select the item "Obtain an IP address automatically"



- Select the Tab "Wireless Networks"



- Click the " Properties " of you Access Point.

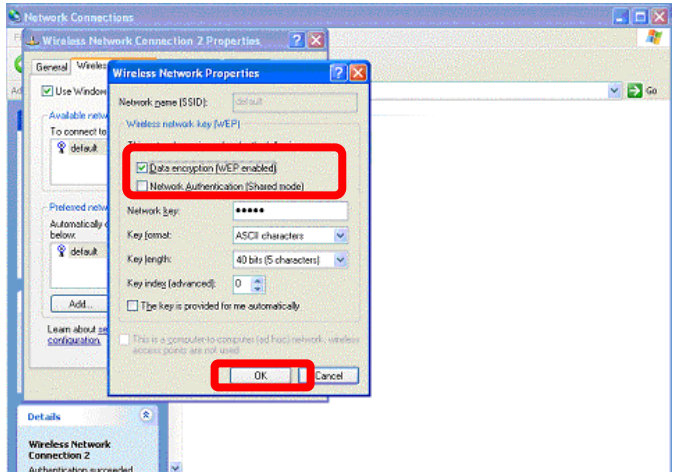
Setup Authentication in client

Setup MD5 authentication in client

In the Properties, you have to choose the **"Data encryption"**

Enter a KEY in WEP mode.

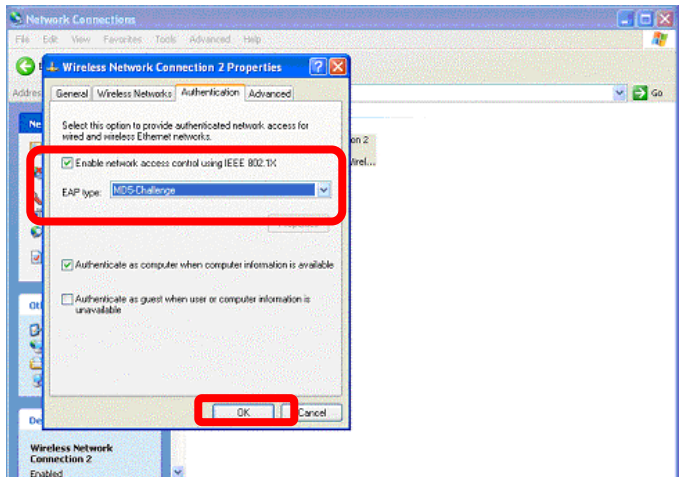
Click **"OK"** Button



Select the Tab **"Authentication"**, please choose **"Enable network access control using IEEE 802.1x"**

Select **"MD5 Challenge"** in EAP type.

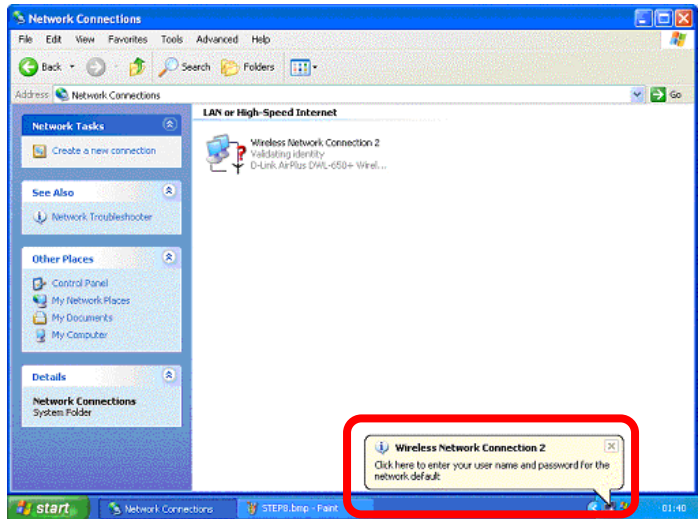
Click **"OK"** Button



Setup Authentication in client

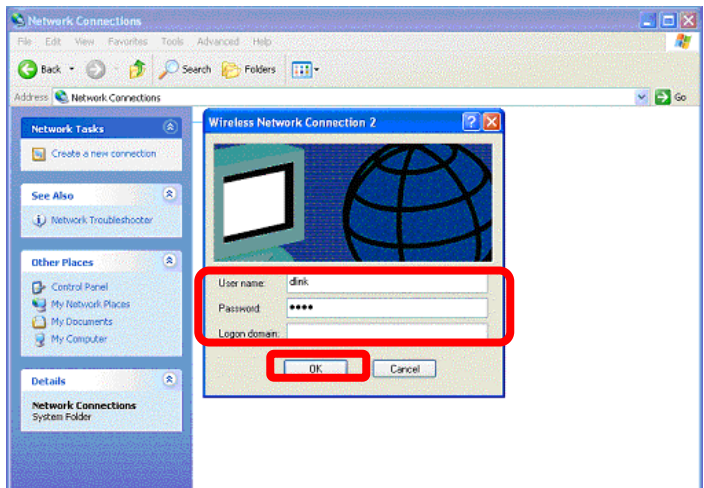
Setup MD5 authentication in client

- Click the yellow, right blow message frame and wait for further authenticating.



- Enter a "User Name" and corresponding "Password"

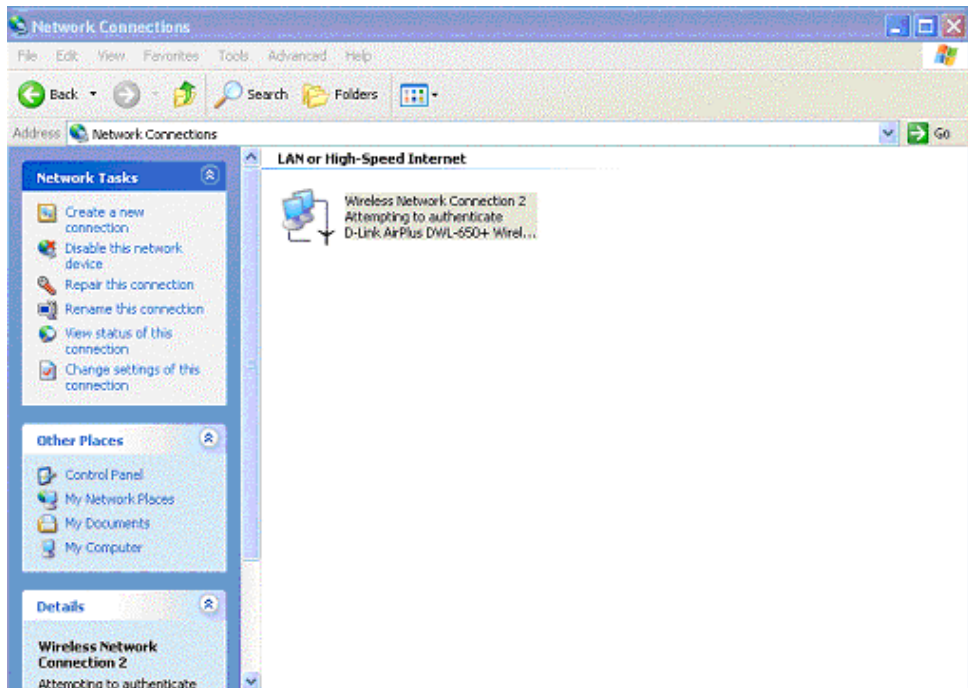
- Click "OK" Button



Setup Authentication in client

Setup MD5 authentication in client

The Authentication was completed.



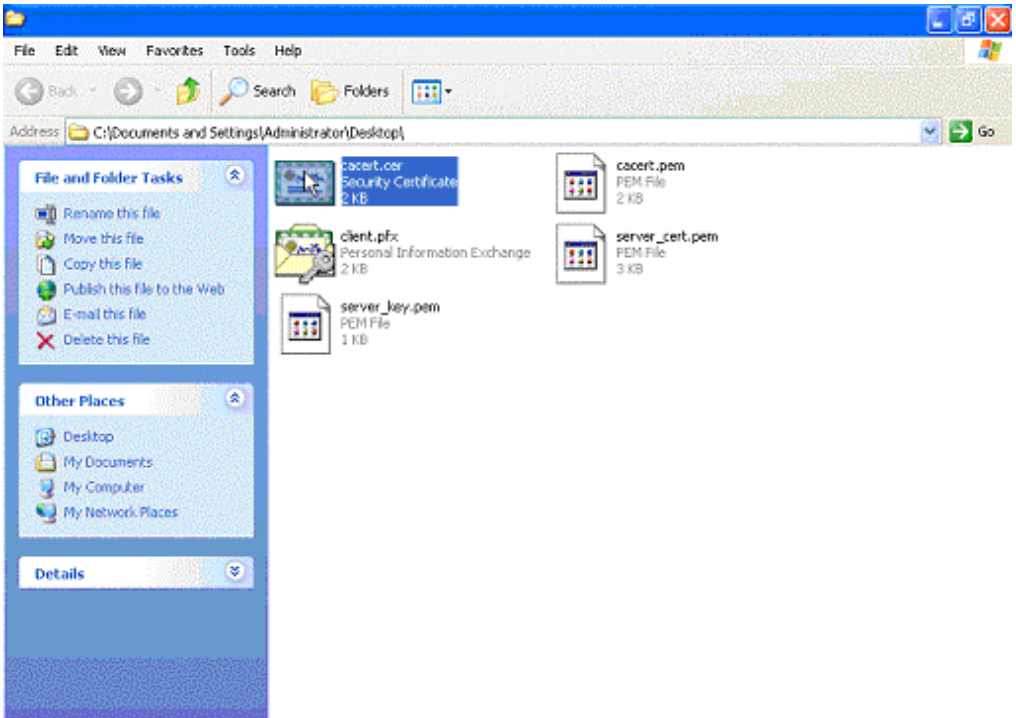
Setup Authentication in client

Setup TLS authentication in client

In Windows Operating System, it's available for TLS authentication in the item "Control Panel". If Client User Certification has been installed, you can carry out the certificate by following steps.

Before you proceeding TLS Authentication, you need to install **"User Certification"**.

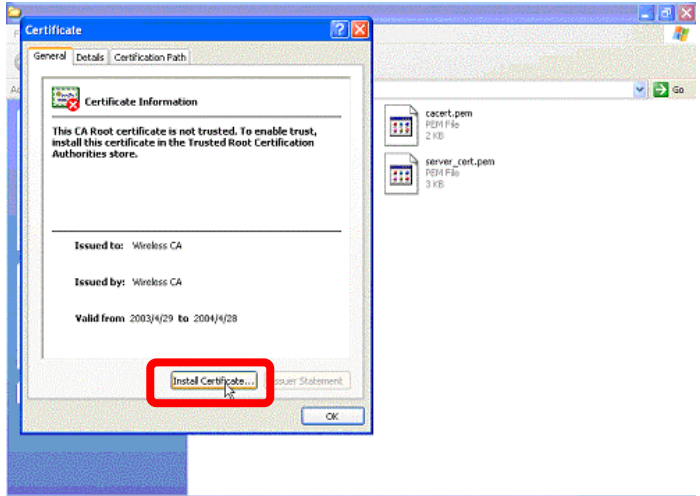
Double click the **" cacert.cer "** file as Security Certification in your folder



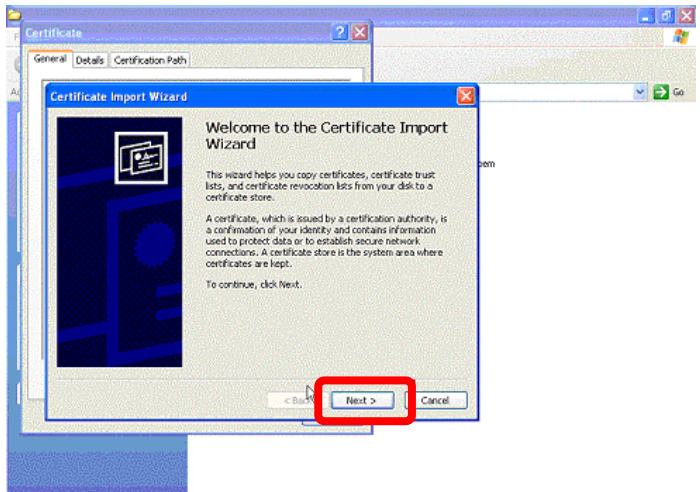
Setup Authentication in client

Setup TLS authentication in client

Click "Install Certificate".



Click "Next".



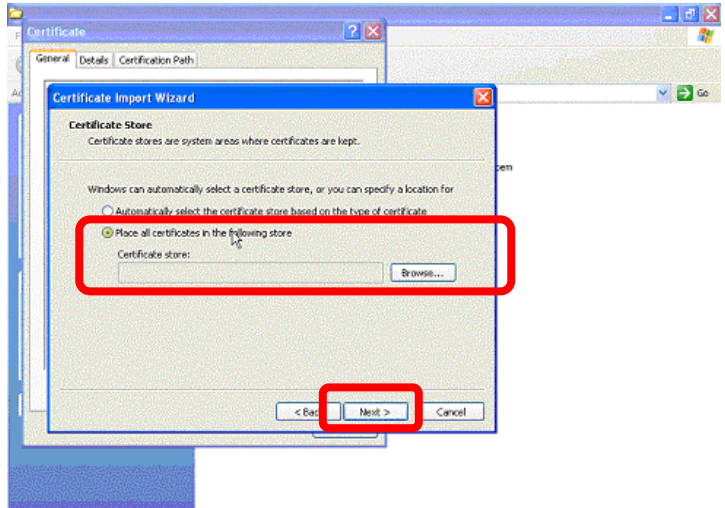
Setup Authentication in client

Setup TLS authentication in client

Choose "Place all certificates in the following store"

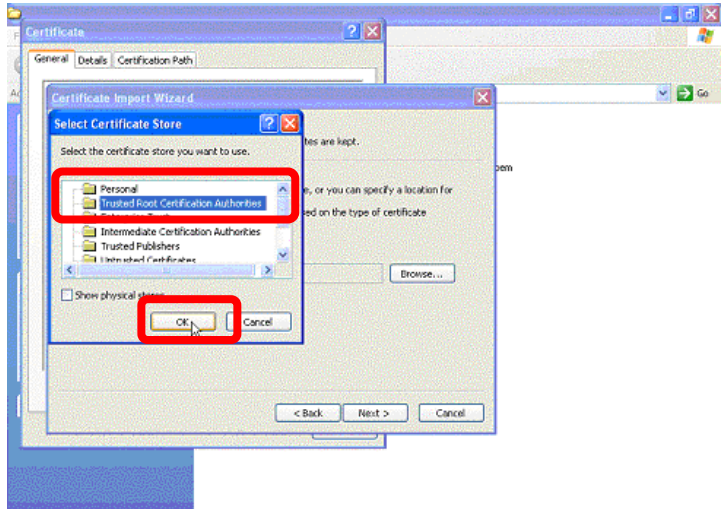
Click "Browse".

Click "Next"



Choose "Trusted Root Certification Authorities"

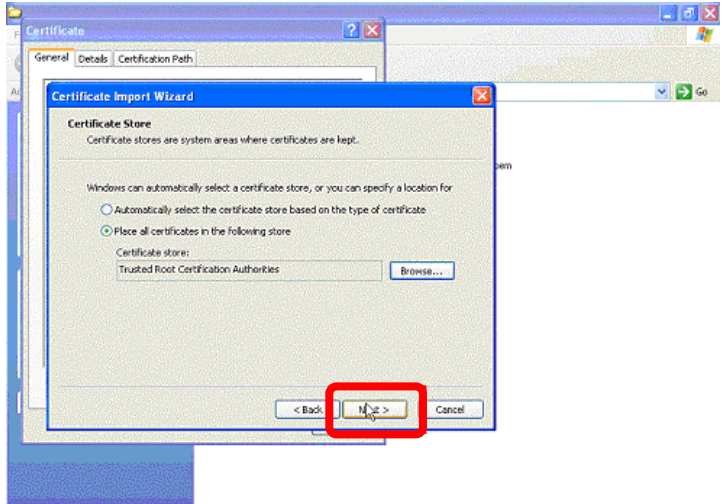
Click "OK".



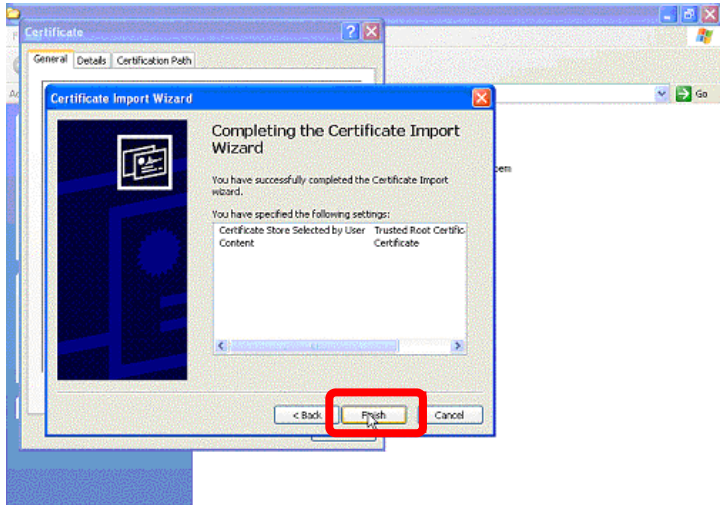
Setup Authentication in client

Setup TLS authentication in client

■ Click “Next”



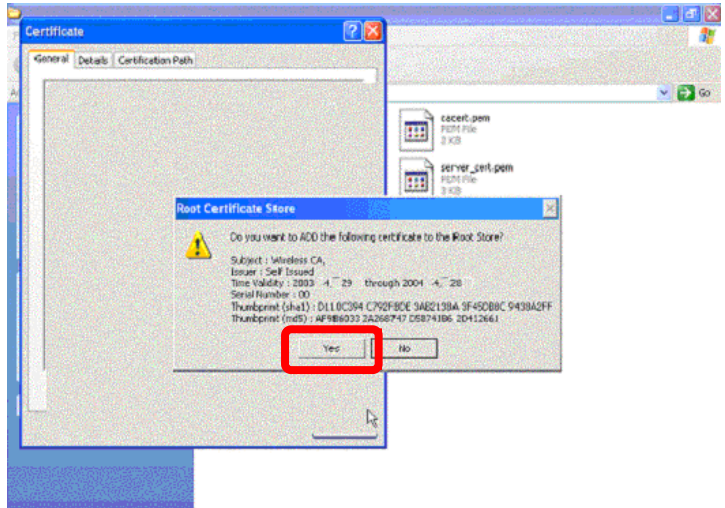
■ Click “Finish”



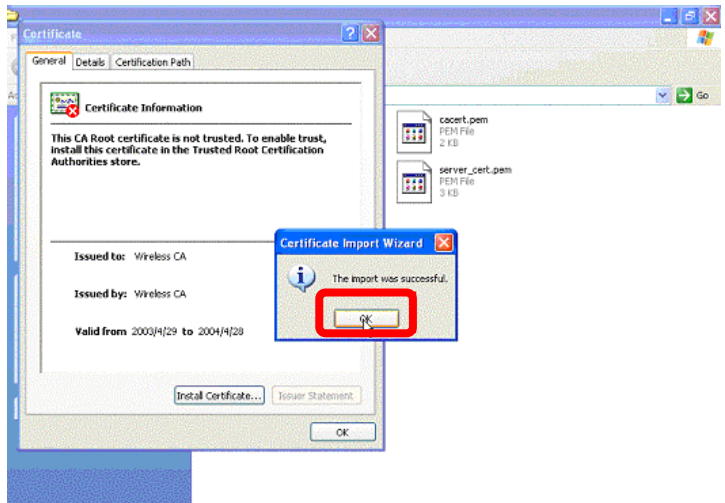
Setup Authentication in client

Setup TLS authentication in client

Click "Yes"



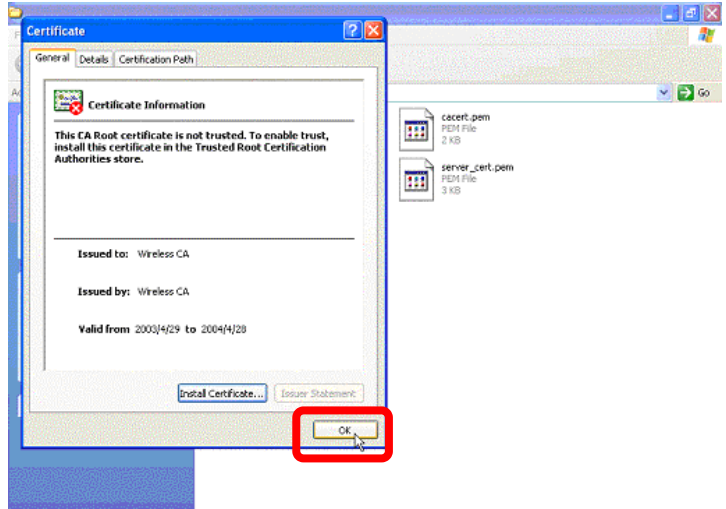
Click "OK"



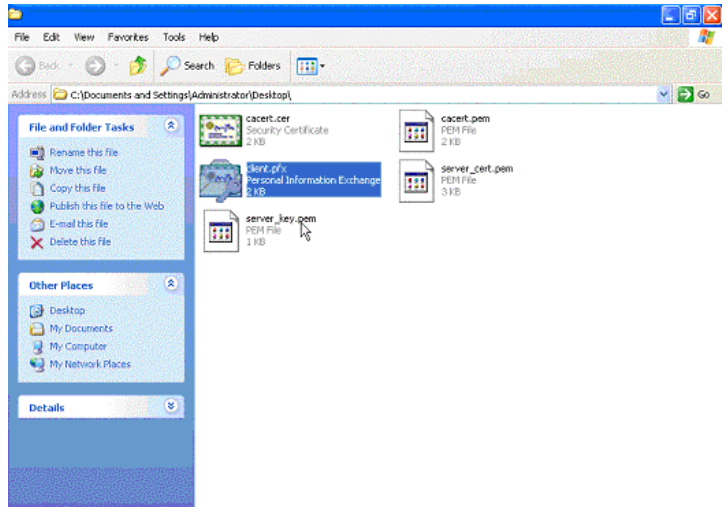
Setup Authentication in client

Setup TLS authentication in client

Finally, click "OK" to finish CA installation.



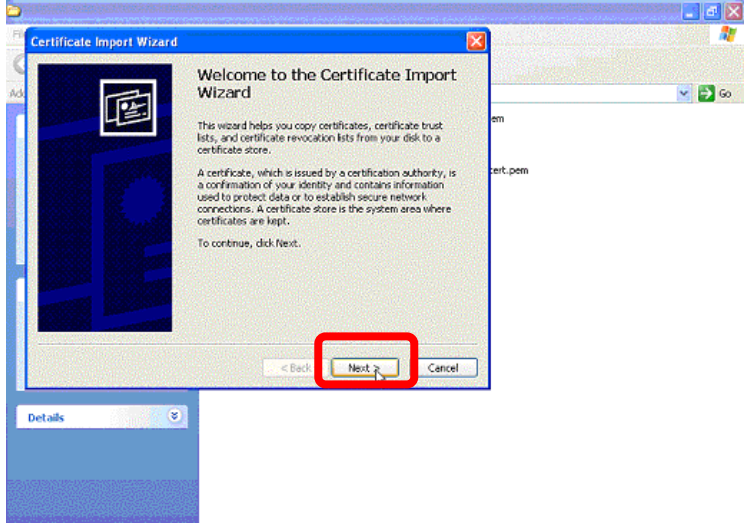
Then Double Click "client.pfx" file as Personal Information Exchange in your folder.



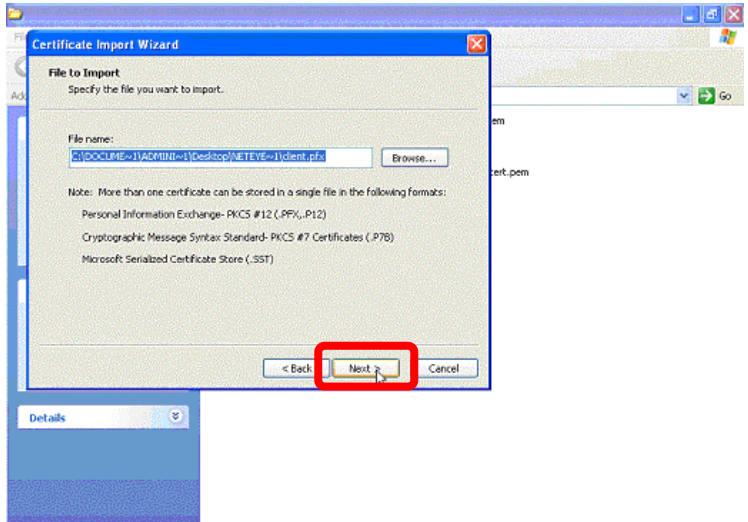
Setup Authentication in client

Setup TLS authentication in client

Click "Next"



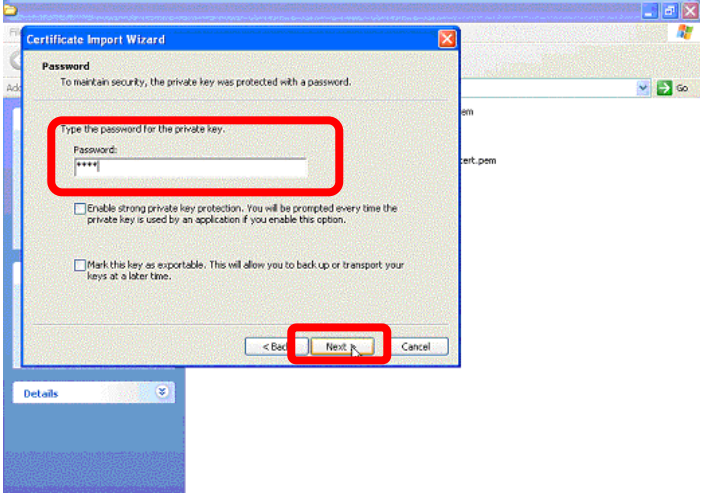
Click "Next"



Setup Authentication in client

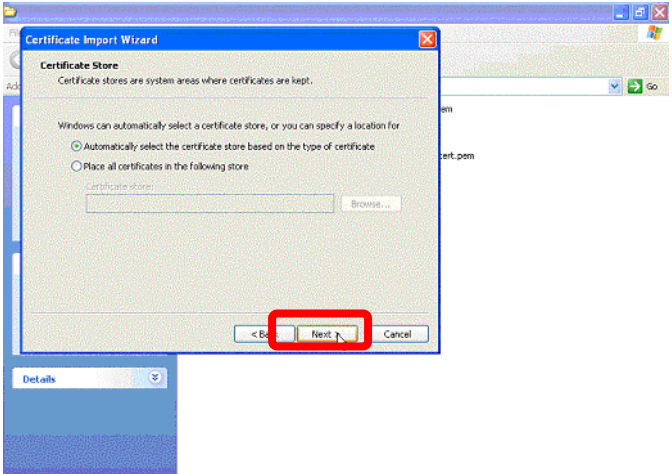
Setup TLS authentication in client

■ Please enter the password of this Authentication



■ Click "Next"

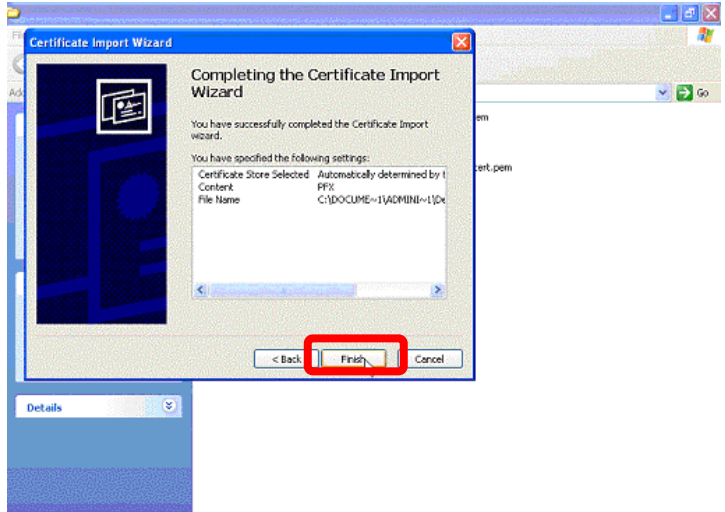
■ Click "Next".



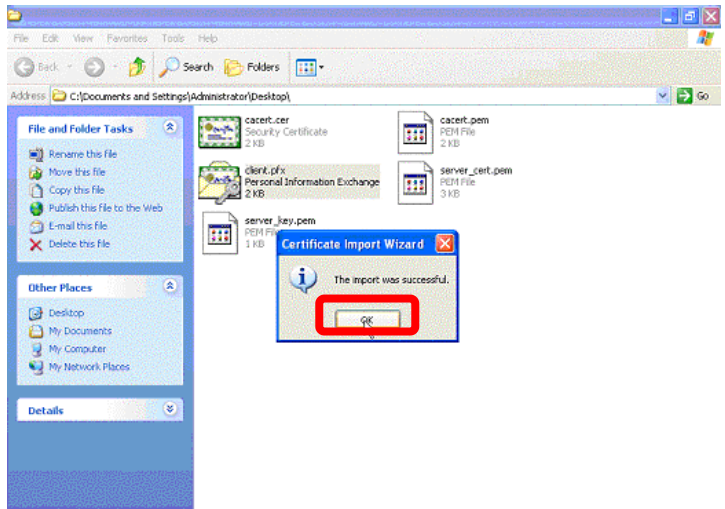
Setup Authentication in client

Setup TLS authentication in client

Then click "Finish".



Finally, click "OK" to finish the installation of Personal Information Exchange.

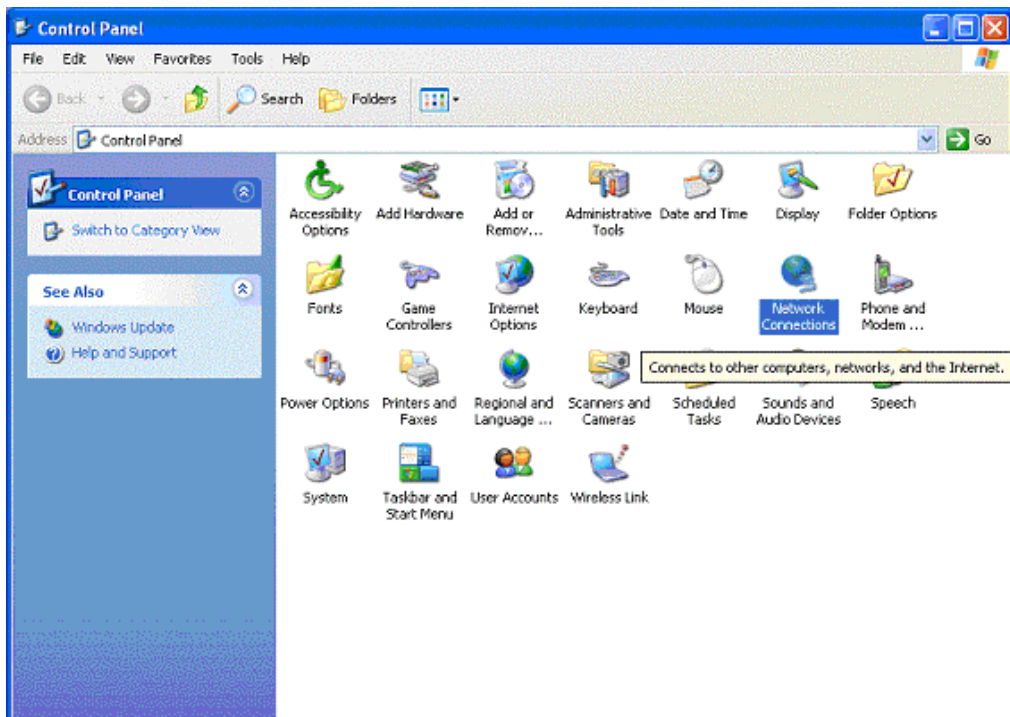


Setup Authentication in client

Setup TLS authentication in client

Now, you can setup the TLS Authentication.

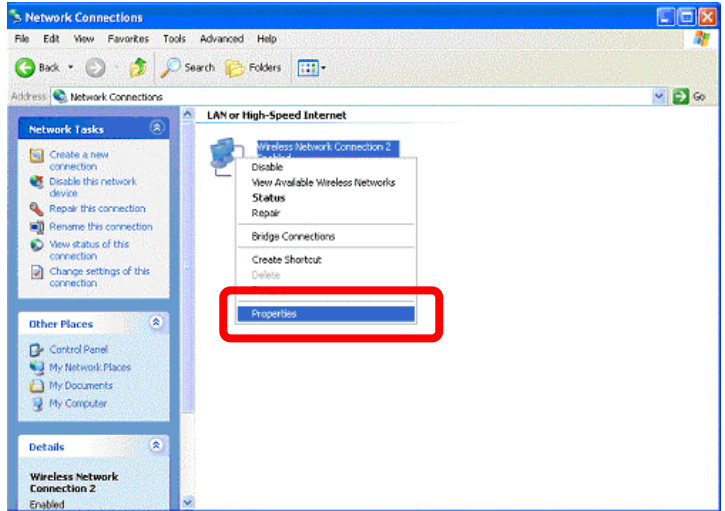
- Go to **Start Click Start (in the lower left corner of the screen)**
- Select **Control Panel** and click
- After open, select **Network Connections** and click



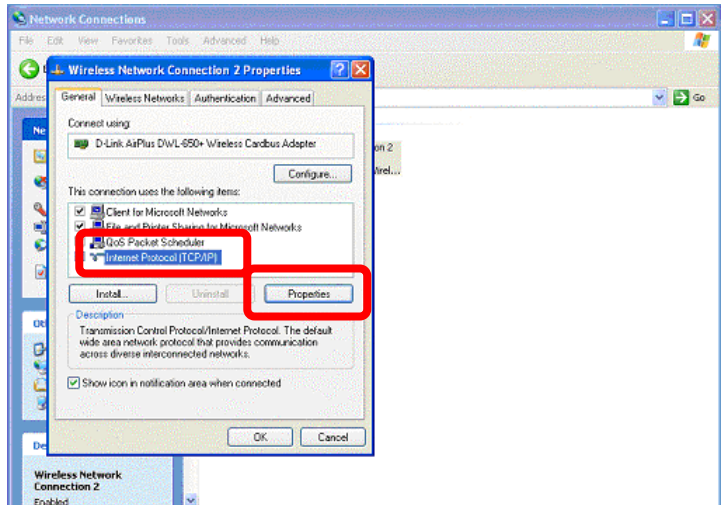
Setup Authentication in client

Setup TLS authentication in client

- Select "Properties" on "Wireless Network Connection" Icon.



- When the dialogue window "Wireless Network Connection Properties" pops up



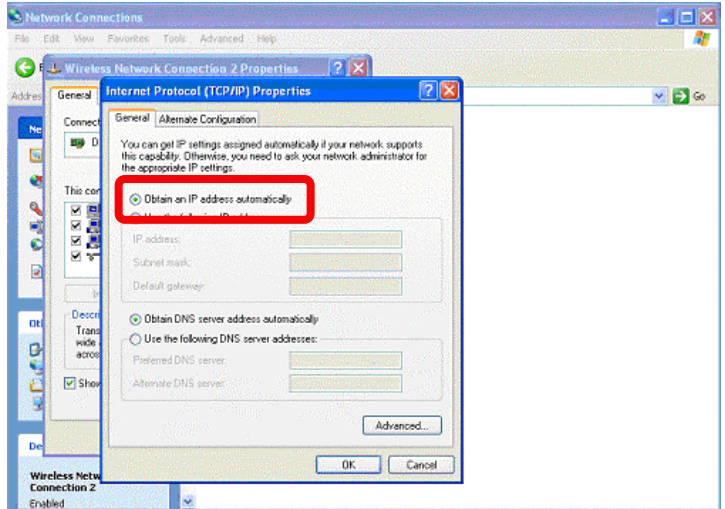
- Choose "Internet Protocol (TCP/IP)"

- Click "Properties"

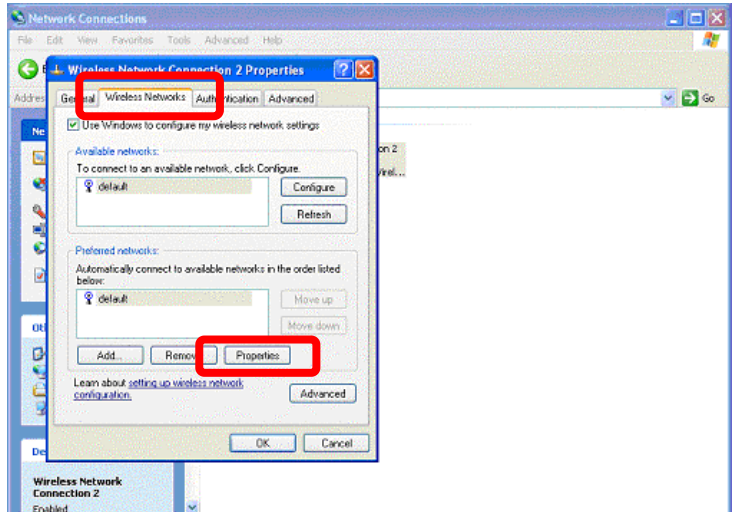
Setup Authentication in client

Setup TLS authentication in client

- Select the item "Obtain an IP address automatically"



- Select the Tab "Wireless Networks"



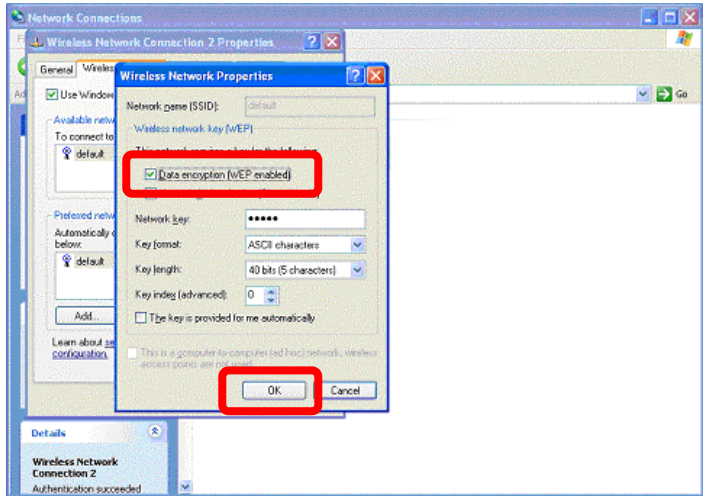
- Click the "Properties" of you Access Point.

Setup Authentication in client

Setup TLS authentication in client

■ In the Properties, you have to choose the **"Data encryption"** and enter a KEY in WEP mode.

■ Click **"OK"** Button

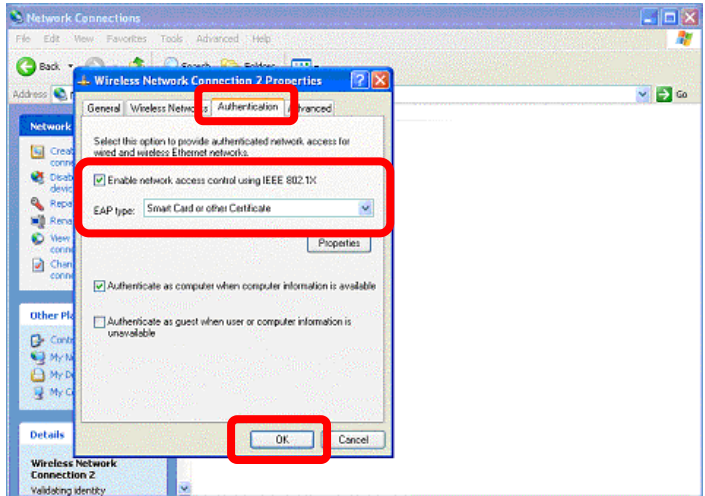


■ Select the Tab **"Authentication"**

■ Choose **"Enable network access control using IEEE 802.1X"**

■ Select **"Smart Card or other Certificate"** in EAP type

■ Click **"OK"**

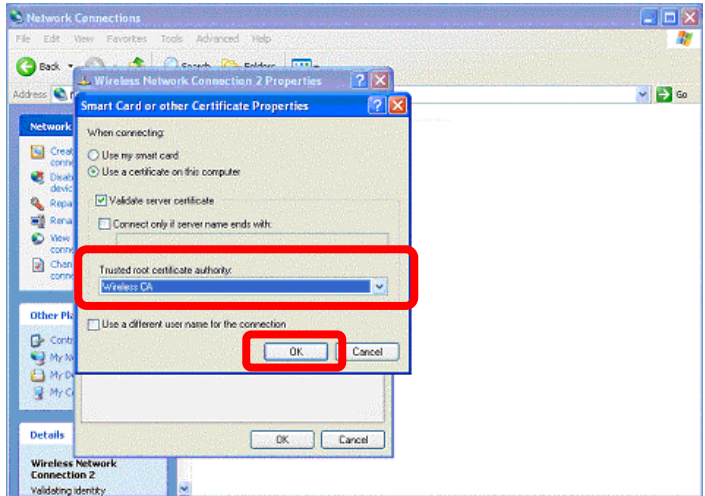


Setup Authentication in client

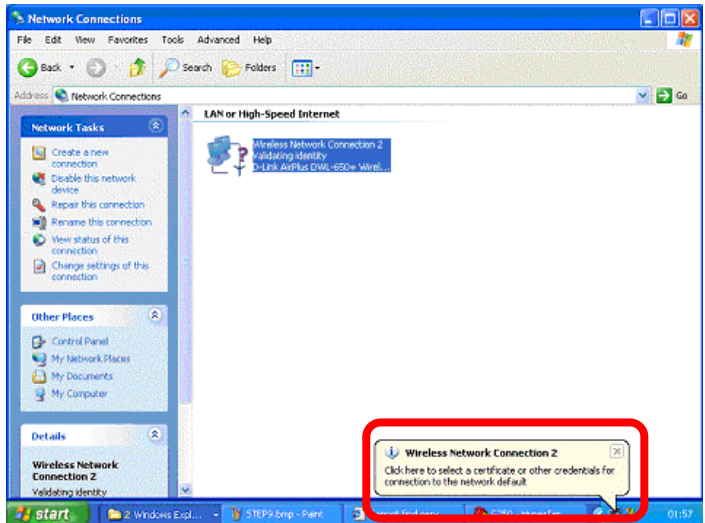
Setup TLS authentication in client

Choose "Trusted root certificate authority" item and select **Wireless CA**.

Click "OK"



Click the yellow, right blow message frame and wait for further authenticating

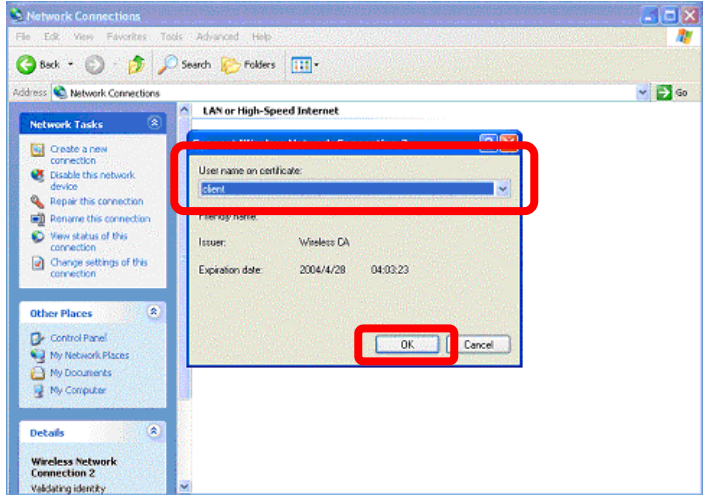


Setup Authentication in client

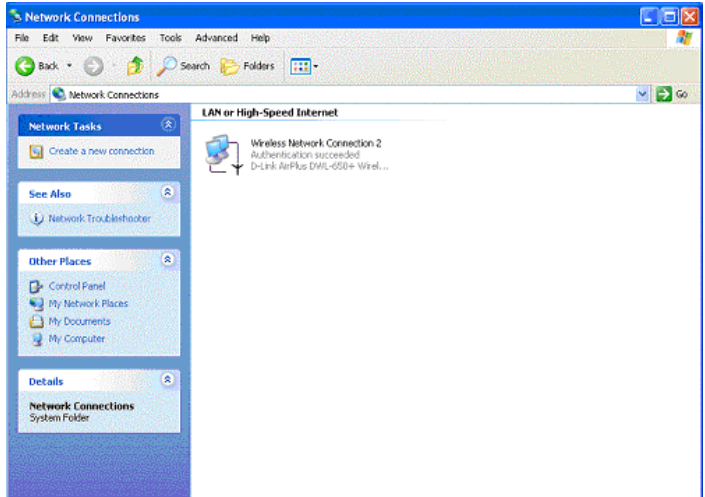
Setup TLS authentication in client

Select the correct target for certificating. This case is an authentication for Client, so "client" is supposed to be selected.

Click "OK"

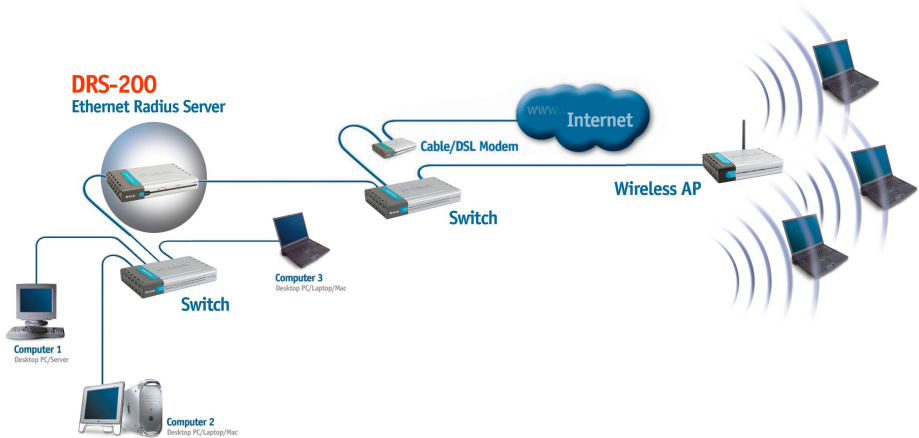


The Authentication was completed.



Connecting Additional Computers To The DRS-200

When you want to DRS-200 be a bridge device. You can using additional Ethernet (CAT5 UTP) cable, connect your Ethernet-equipped computers to the remaining **Local Network port** on the back panel of the DRS-200 via Hub or Switch (like **Hub/Switch2 of legend**). The Local Network port LED will illuminate to indicate proper connection.



In bridging networks, computer or node addresses have no specific relationship to location. For this reason, messages are sent out to every address on the network and accepted only by the intended destination node. Bridges learn which addresses are on which network and develop a learning table so that subsequent messages can be forwarded to the right network.

Bridging networks are generally always interconnected local area networks since broadcasting every message to all possible destinations would flood a larger network with unnecessary traffic. For this reason, router networks such as the Internet use a scheme that assigns addresses to nodes so that a message or packet can be

forwarded only in one general direction rather than forwarded in all directions.

Resetting the DRS-200 to the Factory Default Settings

After you have tried other methods for troubleshooting your network, you may choose to **Reset** the DRS-200 to the factory default settings.



To hard-reset the D-Link DRS-200 to the Factory Default Settings, please do the following:

- Locate the **Reset** button on the back of the DRS-200
- Use a paper clip to press the **Reset** button
- Hold for about 3 seconds (don't hold too long) and then release.
- After you have completed the above steps, the DRS-200 will be reset to the factory default settings and you can re-login.

Contacting Technical Support

You can find the most recent software and user documentation on the D-Link website.

D-Link provides free technical support for customers within the United States for the duration of the warranty period on this product.

U.S. customers can contact D-Link technical support through our web site, or by phone.

D-Link Technical Support over the Telephone:

(877) 453-5465

24 hours a day, seven days a week.

D-Link Technical Support over the Internet:

<http://support.dlink.com>

When contacting technical support, you will need the information below. (Please look on the back side of the unit.)

- *Serial number of the unit*
- *Model number or product name*
- *Software type and version number*

Warranty and Registration

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. ("D-Link") provides this Limited warranty for its product only to the person or entity that originally purchased the product from:

- D-Link or its authorized reseller or distributor and
- Products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, addresses with an APO or FPO.

Limited Warranty: D-Link warrants that the hardware portion of the D-Link products described below will be free from material defects in workmanship and materials from the date of original retail purchase of the product, for the period set forth below applicable to the product type ("Warranty Period"), except as otherwise stated herein 1-Year Limited warranty for the Product(s) is defined as follows:

- Hardware (excluding power supplies and fans) One (1) Year
- Power Supplies and Fans One (1) Year
- Spare parts and spare kits Ninety (90) days

D-Link's sole obligation shall be to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund at D-Link's sole discretion. Such repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement Hardware need not be new or have an identical make, model or part. D-Link may in its sole discretion replace the defective Hardware (or any part thereof) with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement Hardware will be warranted for the remainder of the original Warranty Period from the date of original retail purchase. If a material defect is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to repair or replace the defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware (or part thereof) that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty: D-Link warrants that the software portion of the product (“Software”) will substantially conform to D-Link’s then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days (“Warranty Period”), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. D-Link’s sole obligation shall be to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link’s functional specifications for the Software or to refund at D-Link’s sole discretion. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Software will be warranted for the remainder of the original Warranty Period from the date of original retail purchase. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

Non-Applicability of Warranty: The Limited Warranty provided hereunder for hardware and software of D-Link’s products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold “As-Is” without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

Submitting A Claim: The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same.

- The original product owner must obtain a Return Material Authorization (“RMA”) number from the Authorized D-Link Service Office and, if requested, provide written proof of purchase of the product (such as a copy of the dated purchase invoice for the product) before the warranty service is provided.
- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the Product and will not ship back any accessories.
- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery (“COD”) is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to **D-Link Systems, Inc., 53 Discovery Drive, Irvine, CA 92618**. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link, with shipping charges prepaid. Expedited shipping is available if shipping charges are prepaid by the customer and upon request.

D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link’s reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

What Is Not Covered: This limited warranty provided by D-Link does not cover: Products, if in D-Link’s judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than DLink; Products that have been

purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product. Repair by anyone other than D-Link or an Authorized D-Link Service Office will void this Warranty.

Disclaimer of Other Warranties: EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability: TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY

Governing Law: This Limited Warranty shall be governed by the laws of the State of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This limited warranty provides specific legal rights and the product owner may also have other rights which vary from state to state.

Trademarks: D-Link is a registered trademark of D-Link Systems, Inc. Other trademarks or registered trademarks are the property of their respective manufacturers or owners.

Copyright Statement: No part of this publication or documentation accompanying this Product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Dlink Corporation/D-Link Systems, Inc., as stipulated by the United States Copyright Act of 1976. Contents are subject to change without prior notice. Copyright© 2003 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

CE Mark Warning: In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Statement: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio / TV technician for help.

Register online your D-Link product at <http://support.dlink.com/register/>