your future life

QnoKey

IPSec VPN USB Mobile Key

English User's Manual

Contents

Product Manual Using Permit Agreement

[Product Manual (hereinafter the "Manual") Using Permit Agreement] hereinafter the "Agreement" is the using permit of the Manual, and the relevant rights and obligations between the users and Qno Technology Inc (hereinafter "Qno"), and is the exclusion to remit or limit the liability of Qno. Users who obtain the file of this manual directly or indirectly, and users who use the relevant services, must obey this Agreement.

Important Notice: Qno would like to remind the users to read the clauses of the "Agreement" before using this product. Unless you accept the clauses of this "Agreement", please return this Manual and product. Downloading or reading of this Manual is regarded as accepting this "Agreement" and the restriction of clauses.

【1】Statement of Intellectual Property

Any text and corresponding combinations, diagrams, interface designs, printing materials or electronic files are protected by copyright of our country, clauses of international copyright and other regulations of intellectual property. When the user copies the "Manual", this statement of intellectual property must also be copied and indicated. Otherwise, Qno regards it as tort and relevant duty will be prosecuted as well.

【2】Authority Scope of the "Manual"

The user may install, use, display and read this "Manual" on the complete set of computer.

【3】User Notice

If users obey the law and this Agreement, they may use this "Manual" in accordance with the "Agreement". The "hardcopy or softcopy" of this Manual is restricted to using for information, non-commercial and personal purpose. Besides, it is not allowed to copy or announce on any network computer. Furthermore, it is not allowed to disseminate on any media. It is not allowed to modify any part of the "file". Using for other purposes is prohibited by law and it may cause serious civil and criminal punishment. The transgressor will receive the accusation possibly.

【4】Legal Liability and Exclusion

【4-1】Qno will check the mistake of the texts and diagrams with all strength. However, Qno, distributors and resellers do not bear any liability for direct or indirect economic loss, data loss or other corresponding commercial loss to users or relevant personnel due to the possible omission.

【4-2】In order to protect the autonomy of the business development and adjustment, Qno reserves the right to adjust or terminate the software / Manual any time without informing users. There will be no further notice regarding the product upgrade or change of technical specification. If necessary, the change or termination will be announced in the relevant block of Qno website.

【4-3】All the set parameters are examples and they are for reference only. You may also purpose your opinion or suggestion. We will take it as reference and they may be amended in the next version.

【4-4】This Manual explains the configurations of all functions for different products of the same series. The actual functions of the product may vary with the models. Therefore, some functions may not be found on the product you purchased.

【4-5】Qno reserves the right to change the file content of this Manual and the Manual content may not be updated instantly. To know more about the updated information of the product, please visit Qno official website.

【4-6】Qno/distributors hereby declares that no liability will be born for any guarantee and condition of the corresponding information. The guarantee and condition include tacit guarantee and condition about marketability, suitability for special purposes, ownership and non-infringement. The name of the companies and products mentioned may be the trademark of the owners. Qno/distributors do not provide the product or software of any third party company. Under any circumstance, Qno/distributors bear no liability for special, indirect, derivative loss or any type of loss in the lawsuit caused by usage or information on the file, no matter the lawsuit is related to agreement, omission or other tort.

【5】Other Clauses

【5-1】The potency of this Agreement is over any other verbal or written records. The invalidation of part or whole of any clause does not affect the potency of other clauses.

【5-2】The power of interpretation, potency and dispute are applicable for the law of Taiwan. If there is any dissension or dispute between users and Qno, it should be attempted to solve by consultation first. If it is not solved by consultation, user agrees that the dissension or dispute is brought to trial in the jurisdiction of the court in the location of Qno. In China Mainland, the "China International Economic and Trade Arbitration Commission" is the arbitration organization.

I. Introduction

QnoKey IPSec VPN USB Mobile Key is a highly secure product from Qno Technology Inc. that is easy to use and maintain. It addresses the needs of enterprises to allow personnel to access applications on corporate VPNs remotely and securely from outside offices.

The QnoKey USB flash drive is designed as lightweight and portable. With the built-in encryption chip and Plug & Play interface, it is not only easy to use but is also equipped with an added layer of protection. With the included client-side connectivity software, just entering the password, you can quickly establish VPN connections. This makes a more user-friendly, secure, and cost-effective VPN connectivity solution possible.

In Qno Router series that have QVM VPN capability, almost all of them support QnoKey connectivity and are able to accept remote connection with a QnoKey. QnoKey can be used with the following operating systems with a high degree of compatibility: Windows 2000 / XP / Vista / Win 7.

Management software works with Qno VPN firewall / router to allow network management to carry out initial user configurations for QnoKey on the management side computer, as well as the Personal Identification Number (PIN) for QnoKey itself. With the QnoKey and PIN, all the user needs to do is to insert the QnoKey into the USB interface of a computer with the software already installed, enter the PIN code, and an IPSec VPN connection will be automatically set up. The product is simple to configure, easy to use, and combined with encryption parameters, realizing a more convenient and more secure VPN connection.

A Comprehensive List of QnoKey Features is Summarized as follows:

※ **Highly security:** The USB hardware has a built-in encryption chip that can bind with the computer, support user authentication and use full IPSec VPN data encryption and authentication. With multiple security checks, it is guaranteed that the key cannot be falsified.

※ **QnoKey client life time can be set:** Upon reaching expiration date, the key will be rendered ineffective to ensure security.

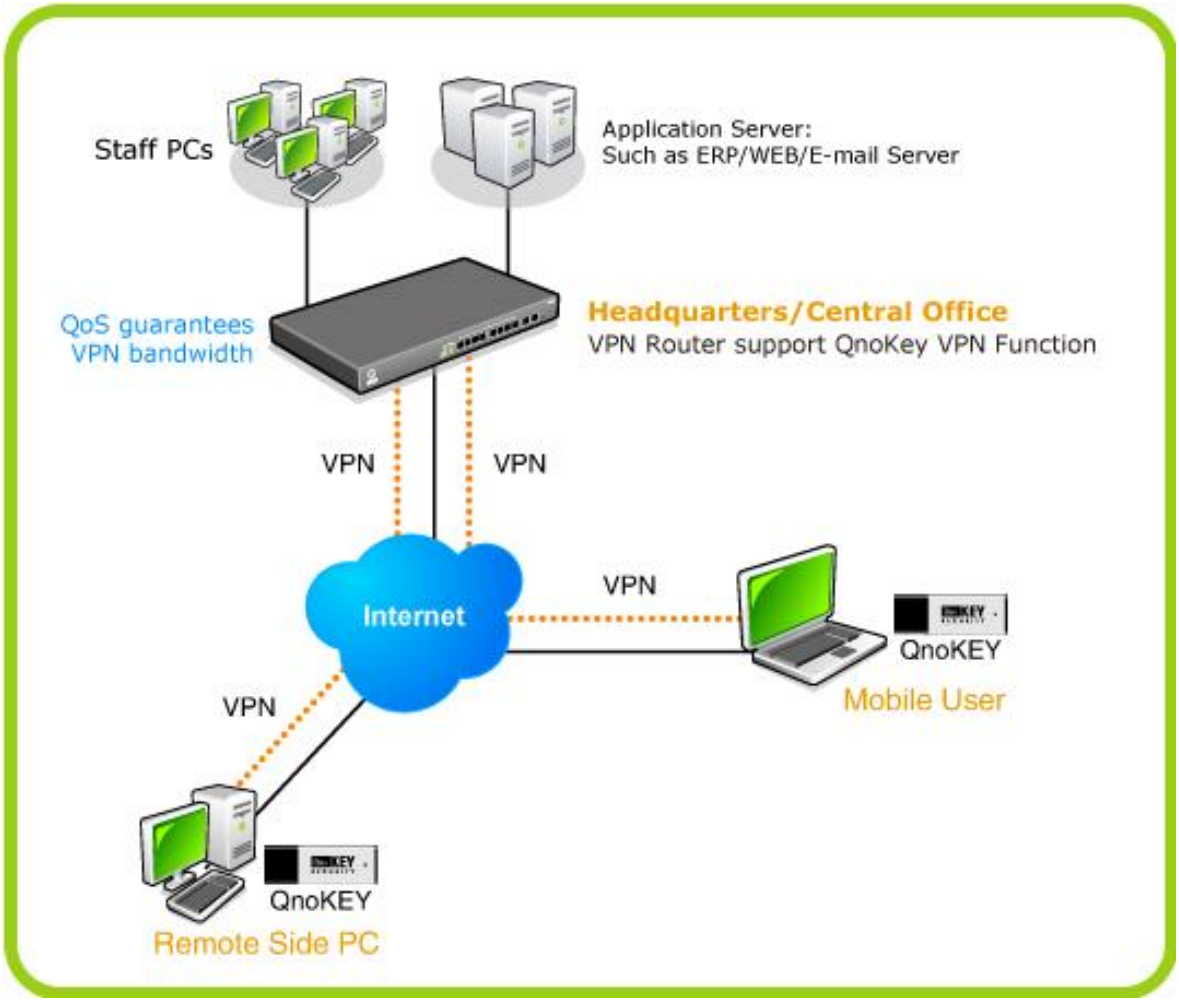
※ **Support for Stolen Key Login Actions:** Able to block connections from a QnoKey already identified as lost, or remove storage parameters of a lost QnoKey automatically to minimize losses. In addition, after each use, all temporary data QnoKey stores on the computer that may present security concerns will be removed. This is a very practical design for users using a public computer, and is an added layer of protection in terms of information security.

※ **Easy to use:** With the Plug & Play USB interface and the included client software, after the QnoKey has been inserted, all the user needs to do is to enter the password in order to connect to the VPN automatically. After the QnoKey client software has been installed, there is no need for the user to perform any configuration tasks. It is possible for users with virtually no knowledge about the network to get started quickly.

※ **Easy to manage:** Supports management at the group level; allows groups to be duplicated to save time and effort. On the router management screen, the connection status of all QnoKey users are clearly displayed so that an enterprise network manager can easily manage enterprise users, servers and application resources centrally, reducing the workload and at the same time achieving better security.

※ **Cost savings:** It can replace the more expensive external node stand-alone VPN networking equipment, thus reducing the cost of VPN deployment significantly. Maintenance-free with no external nodes or equipment to manage, thereby saving on human resources costs.

Product deployment diagram



The features currently supported by the majority of Qno's VPN series products are listed in the following table

Model	QVF8034	QVF8042	QVF8072	QVF8205
QnoKey Max. No. of supported channels	100	200	300	600
Capacity	100~250	300~500	300~500	500~750

Model	QVF8210	QVF8230	QVF7105	QVF7405	QVF7403
QnoKey Max. No. of supported channels	1000	400	100	100	200
Capacity	750~1000	1000~1200	100~200	200~250	300~400

Note: The maximum number of QnoKeys that each model supports can only be achieved after the number of channels used by other VPN-related applications (e.g. IPSec VPN, PPTP, QVM) is decreased to the minimum level (zero-channel).

II. QnoKey Product Specifications

Software Application Specifications:

- USB Plug & Play hardware; to create a VPN connection users only need enter the password

- Supports Windows 2000 / XP / Vista / Win7 Operating Systems

- Uses full IPSec VPN data encryption and authentication, with support for 3DES

- Users can modify password to guard against theft of the QnoKey

- Supports Lost Key Login Mechanism: Able to block connections from a QnoKey identified as lost, or remove storage parameters of the lost QnoKey automatically

- Management will be able to duplicate the set of connection parameters for a group and distribute it to different users to reduce the otherwise repetitive configuration efforts.

- Management will be able to set the connection life time for each QnoKey to prevent improper use.

- Management will be able to set multiple WAN IP connections for backup purposes.

- Management will be able to display the connection records of each QnoKey user, effectively monitoring the connection status.

Hardware Specifications:

The hardware supports the standard USB interface, has passed Microsoft Windows Hardware Quality Labs (WHQL) testing, and uses DES to store data from being stolen.

Operating voltage: 2.2 - 5.5V

Operating current: <150mA

Operating temperature: 0℃ - 70℃

Storage temperature: -40℃ - 85℃

External dimensions: 49mm × 17.2 mm × 7mm

Weight: 8.5 g

III. Deployment Configurations

This chapter describes the deployment of QnoKey, its connection requirements and environment, as well as the configuration process.

3.1 Requirements for the Installation and Operating Environment of the Connectivity Software

Before install QnoKey, the application suite performs the necessary configuration, please check your computer system to see if it meets the following requirements:

A. Your computer's operating system must be one of the following:

Windows 2000

Windows XP

Windows 2003

Windows Vista

Windows 7

B. Your computer must have one or more unused USB ports

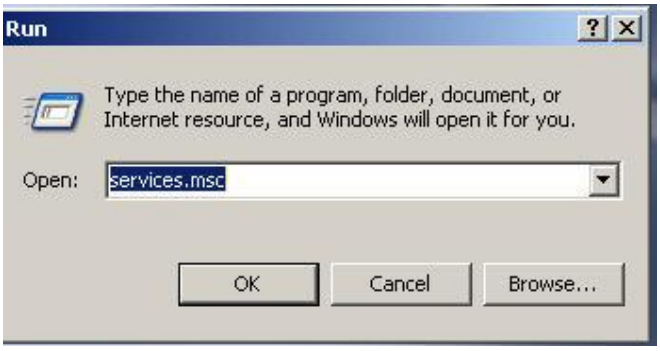
※ Notice! Please log on as Administrator (the user with maximum level of authorization) on the computer for software installation. For Vista users, before attempting to install QnoKey software, go to "Control Panel" => "User Accounts"=> "Disable User Account Control."

C. Please check whether or not your Qno firewall / router supports QnoKey functionality. If it does not, you will not be able to use QnoKey to connect VPN.

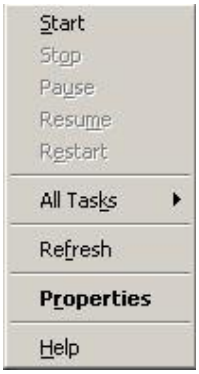
D. Under Windows operating system, confirm that the following steps are completed:

(1) Start "Smart Card" service and configure it to start automatically upon system start-up. The example below uses Windows Vista for illustration

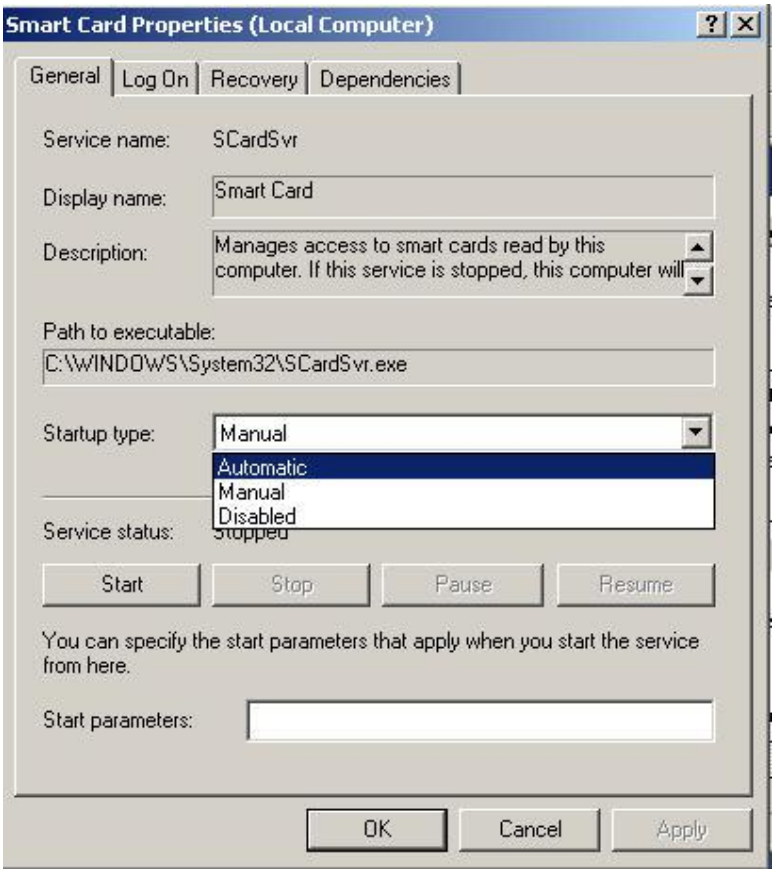
=> Start => Run => Type in "services.msc" to enter into “Service Manager” (Please note that only users with Administrative privileges can enter into the “Service Manager”)



=> Enter service management, locate the "Smart Card" service and then right-click and select "Properties" from the menu, as shown in the diagram below.

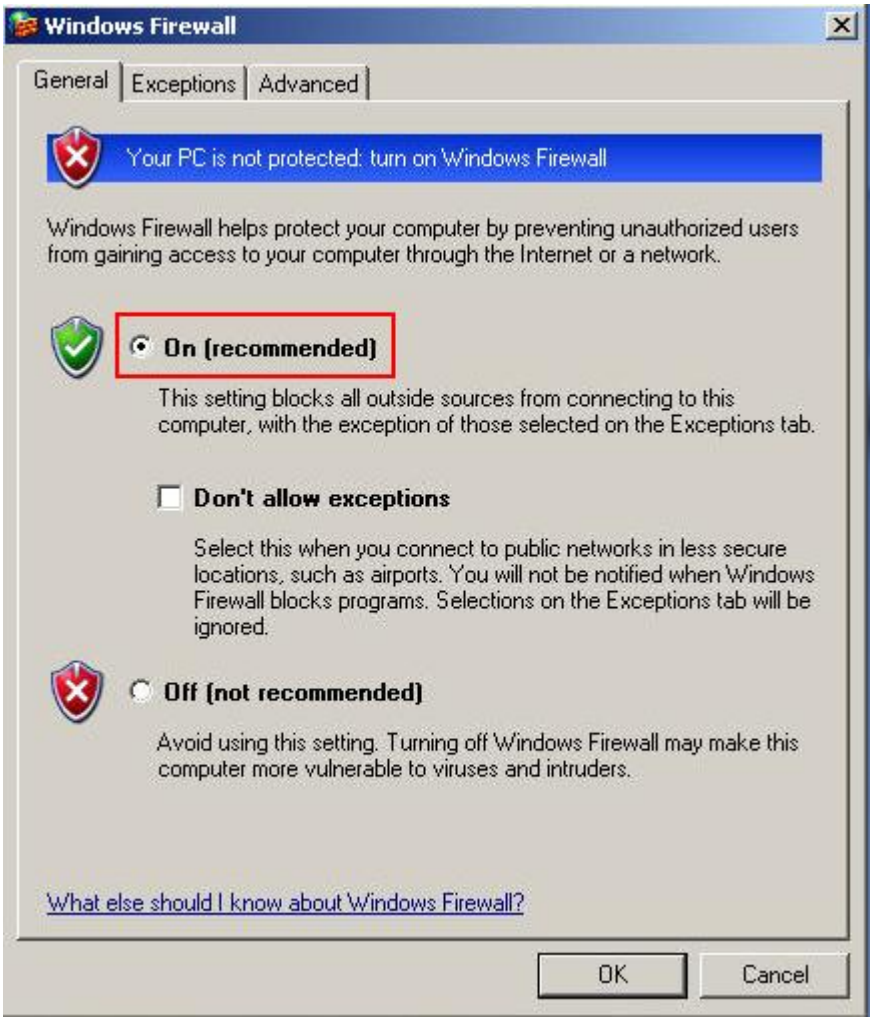


After clicking on the properties, select "Automatic" under "Startup type" and click on "OK" to confirm. Restart the computer so that each time the computer starts, Smart Card service will start automatically and becomes a service that is required for QnoKey.

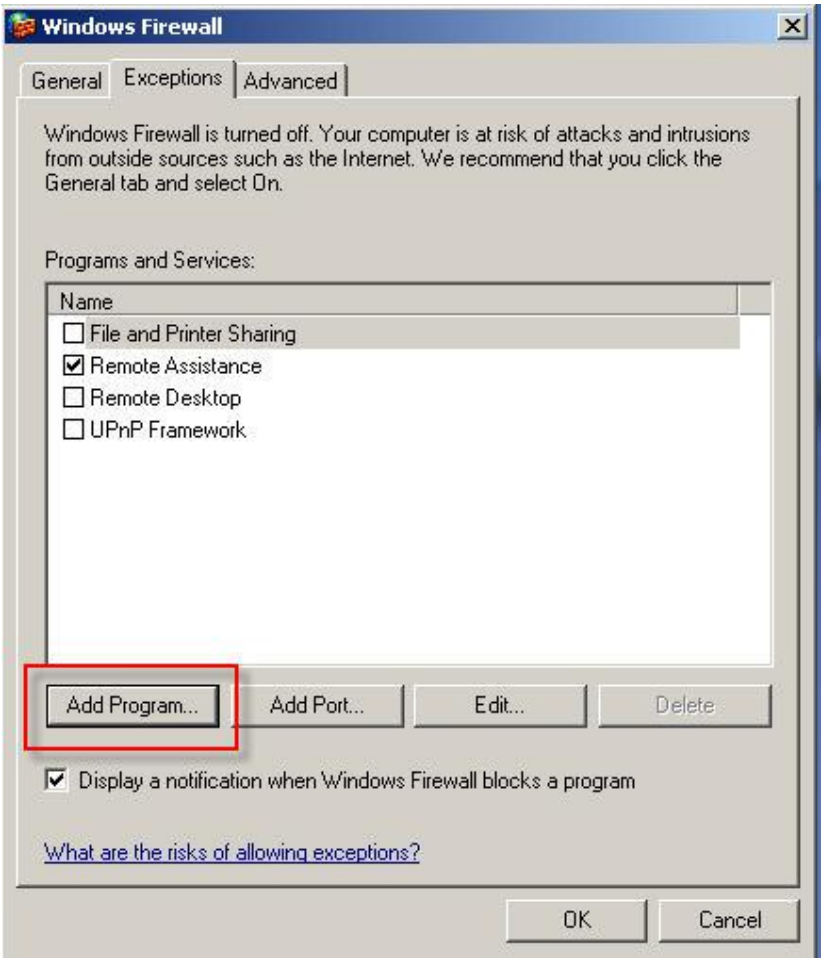


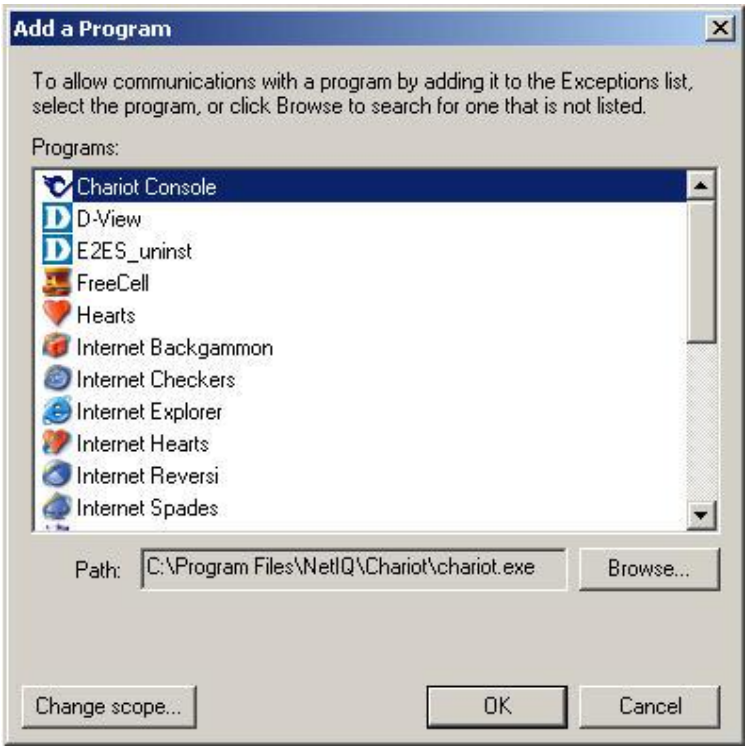
(2) Enable Windows Firewall and permit QnoKey to pass through.

=> Settings => Control Panel => Windows Firewall => Choose “On” to enable the firewall



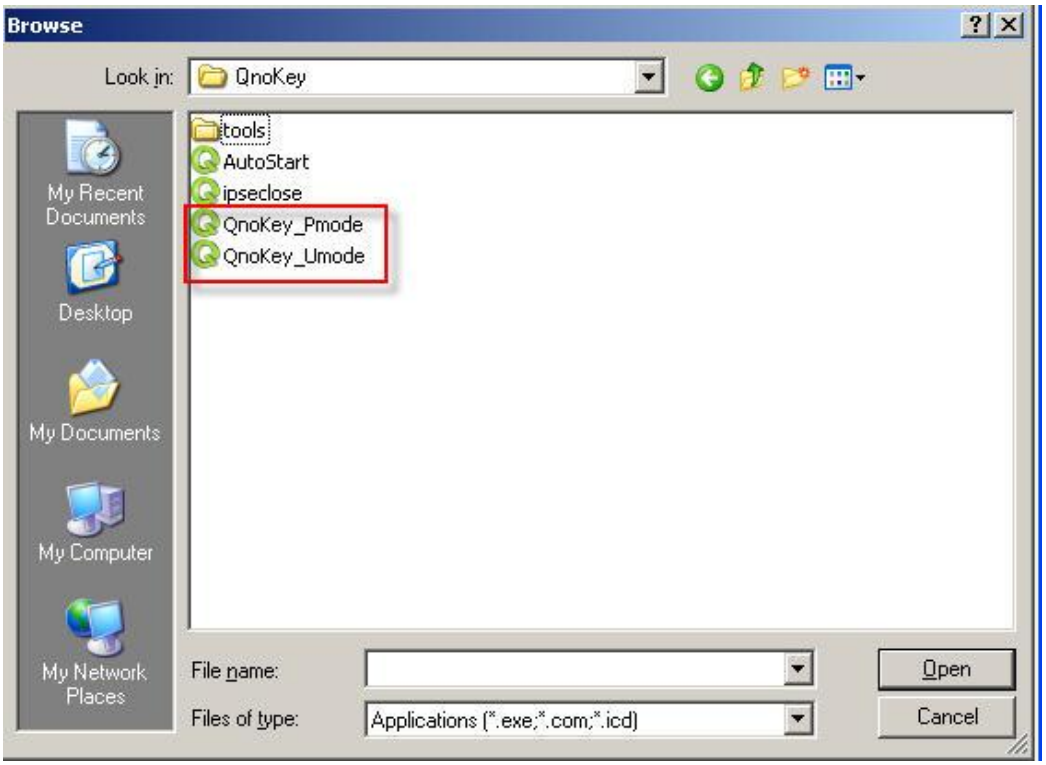
=> On the Exceptions tab, press "Add Program...", locate QnoKey in the list, and add it to the Exceptions list (the QnoKey management software or user connection software must have been installed with Administrator privileges before added to the list)


Windows Firewall
General
Exceptions
Advanced
Windows Firewall is turned off. Your computer is at risk of attacks and intrusions from outside sources such as the Internet. We recommend that you click the General tab and select On.
Programs and Services:
Name
File and Printer Sharing
Remote Assistance
Remote Desktop
UPnP Framework
Add Program...
Add Port...
Edit...
Delete
Display a notification when Windows Firewall blocks a program
What are the risks of allowing exceptions?
OK
Cancel


Add a Program
To allow communications with a program by adding it to the Exceptions list, select the program, or click Browse to search for one that is not listed.
Programs:
Chariot Console
D-View
E2ES_uninst
FreeCell
Hearts
Internet Backgammon
Internet Checkers
Internet Explorer
Internet Hearts
Internet Reversi
Internet Spades
Path:
C:\Program Files\NetIQ\Chariot\chariot.exe
Browse...
Change scope...
OK
Cancel

If it is not on the list, click Browse, locate QnoKey's executable file under the installation folder. Select it and add it to the firewall's Exceptions list.

(The installation path is usually C:\ProgramFiles\Qno\QnoKey, where Pmode is the executable file of the QnoKey management software, Umode is QnoKey user's executable for connection. It is recommended that both be added to the list)



(3) Disable the computer's antivirus software or the firewall that comes with the antivirus software. If you do not wish to disable it, you will have to add QnoKey to the exceptions list of the antivirus software or the firewall that comes with it. Consult the software vendor's manual for how this can be done.

※ Please note!

In the event that there are other antivirus softwares, firewalls that come with antivirus software, specialized firewalls or other applications other than those provided by Windows that cause QnoKey to fail to make VPN connections, while Qno technical support staff or customer service personnel will do their best to assist you in configuring your system, we cannot guarantee that a connection can always be made, or that there will be no subsequent problems. Please consult the relevant software vendors for compatibility issues.

3.2 Configuration Procedures

Follow the installation procedures:

1. Initial configuration for QnoKey group information can be done through the software management interface of the firewall / router

Through Qno firewall / router configuration UI the Network Administrator can carry out the initial configurations about information in QnoKey client-user.

2. Data is written to QnoKey via the QnoKey management software and the PIN (personal / user identification code) is set:

Through the QnoKey management software, the QnoKey PIN is set. The data required to establish IPSec VPN connection in the firewall / router is written to QnoKey and the QnoKey is burnt successfully.

3. Preparations before dialing up the VPN:

After configuring the QnoKey account, the Network Administrator can return the QnoKey and PIN to the mobile user; meanwhile install the client connectivity software on the CD-ROM for the mobile user.

4. Using QnoKey software in client-user to establish VPN connection:

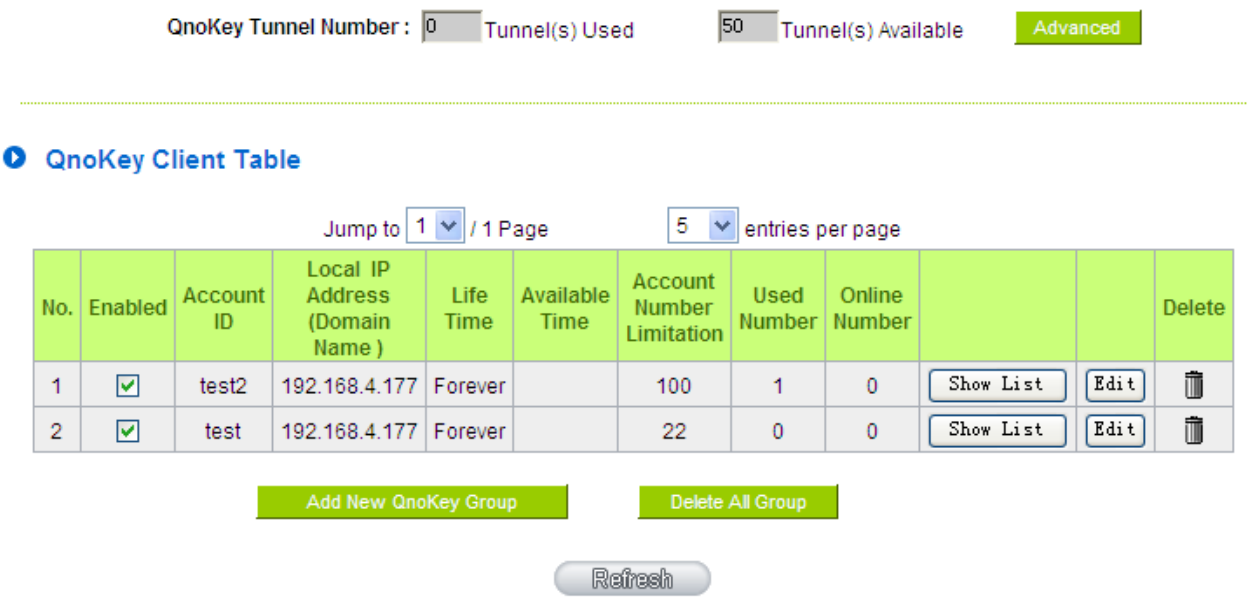
The user all needs to do is to insert QnoKey into the USB port in an installed computer and enter the PIN, and the IPSec VPN connection will be established automatically.

IV. QnoKey Group Setting and Management

This chapter mainly focuses on how to conduct initial user data configuration and group management settings in Qno firewall / router equipment.

4.1 QnoKey Main Configuration Screen

After Logging into the Qno firewall / router, click to open the QnoKey menu options to view the current QnoKey status summary screen, as shown below:



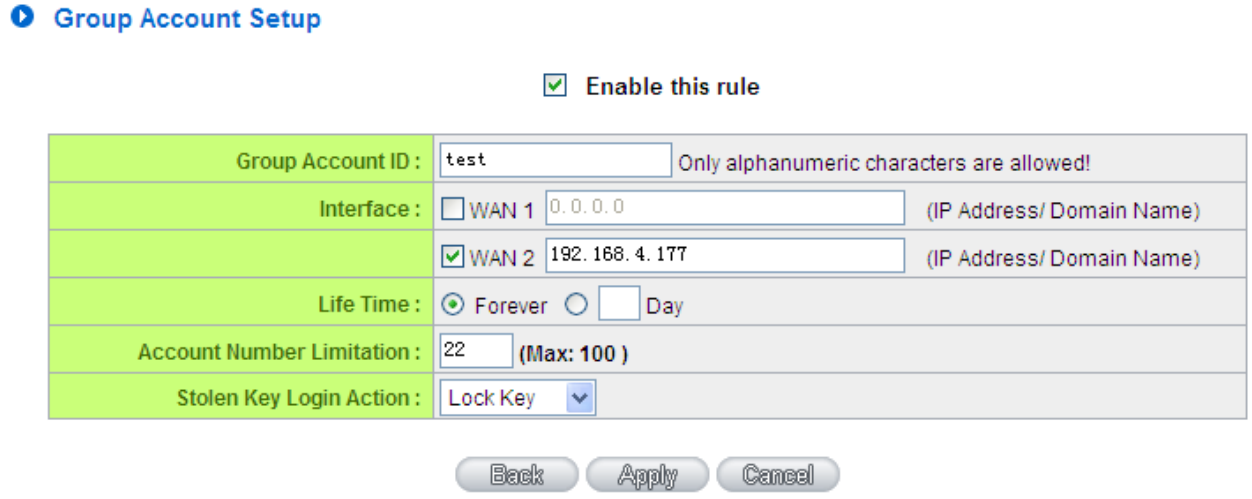
QnoKey Tunnel Number	This shows the number of tunnels that have been configured and used, and the number of tunnels currently available. Clicking the "Advanced settings", users can adjust IPSec VPN, QnoKey, PPTP and QVM tunnel number themselves.

QnoKey Client Table summary	
Enabled:	This shows if the QnoKey user group is enabled.
Account ID:	This shows the name of the QnoKey user group.
Local IP address (Domain Name):	This is the IP address of the QnoKey server or the domain name used. (Generally referring to the WAN IP of the current router / firewall)
Life Time:	This sets the expiration of the QnoKey. For permanent, unrestricted use, "Forever" will be shown here.

Available Time:	After setting QnoKey's life time, this will show the remaining time available.
Account Number Limitation:	This represents the maximum allowable number of USB keys that can be written (burned) by this user group.
Used Number:	This represents the number of USB keys that have been written (burned) with administration / connection data.
Online Number:	This shows the number of QnoKey users currently connected.
Show List:	This displays the list of all QnoKey users that have been configured.
Edit:	The properties of the user group can be modified by clicking on the "Edit" button.
Delete	Delete all settings of this user group.
Add New QnoKey Group:	Add a new group
Delete all groups:	Clear and remove the settings for all groups.
Refresh:	Clicking on this button, it will represent the updating status of all group settings and current online connection.

4.2 Group Account Setup Screen

Click "Add QnoKey Group" to enter "Group Account Setup", as shown below.



This page is mainly used for setting up the QnoKey group. Here QnoKey group parameter settings such as WAN port, Life Time, Account Number Limitation, Stolen Key Login Action and so on can be set via the

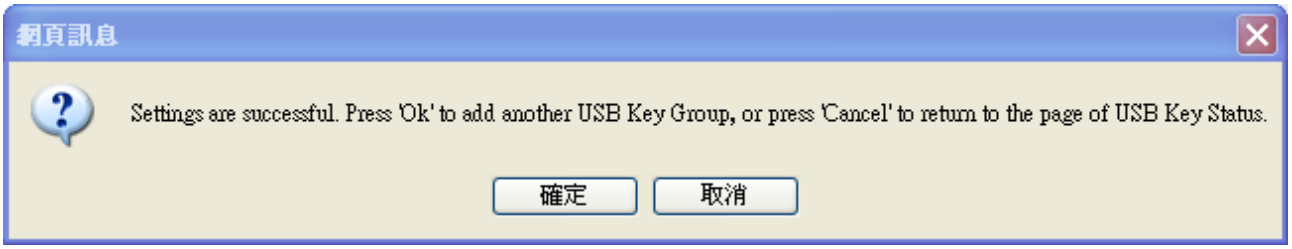
WAN port in order to perform management and classification on QnoKey users and to improve security.

Enable this rule:	Checking this option will enable the settings for this group.
Group Account ID:	Type in the name of the QnoKey group you want to set up
Interface:	Check to configure the WAN port desired and fill in the IP address or domain name for the corresponding WAN port. If the WAN port is blank, then the IP address is not required; otherwise this may prevent the VPN from being connected. The purpose is to designate which WAN port used for VPN connections, which facilitates administration. If WAN 1 is selected, this QnoKey group user can only connect to the VPN via WAN 1. If WAN 1 and WAN 2 are simultaneously selected, this QnoKey group user can connect to the VPN via WAN 1 or WAN 2. In the event that WAN 1 is disconnected, the system will be automatically switched to WAN 2 as a backup. **※ Please note:** ■ If the selected WAN port has a fixed IP (with a designated IP address), the system will automatically show this WAN IP and the administrator need not enter anything. ■ If the selected WAN port follows DHCP/PPPoE or other ways, then the administrator has to enter the correct IP address or domain name.
Life Time:	Set up the life time for this QnoKey group here. If the client is a regular user, network administrator can select "Forever" for a permanent usage If the situation is more complicated, or if the QnoKey is

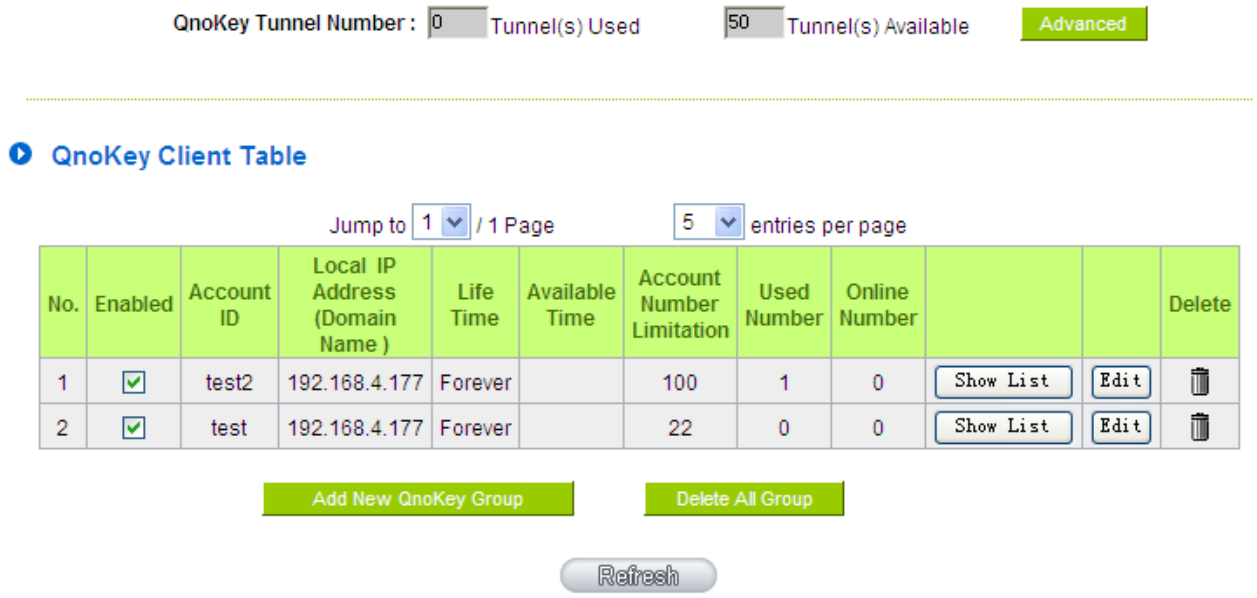
	provided for mobile users on business trips, to ensure a secure VPN, the administrator may set the life time for the QnoKey just a few days. Here the range is from1 to 99 days. The exact desired number of days can be entered here.
Account Number Limitation:	This represents the maximum allowable number of USB keys that can be written (burned) by this user group. (There is a maximum of 100 online users limited for each group)
Stolen Key Login Action:	On the drop-down menu, select the action desired for a lost or stolen QnoKey. If the QnoKey is lost by accident, there are three possible actions available (1) No protection: Take no restrictive actions after lost. (2) Clear Key content: If a VPN connection is established after the QnoKey has been lost, the data associated with this QnoKey will be deleted. (3) Prohibit connection: The QnoKey will be blocked and locked out after it is lost and cannot be used to access the VPN.

Press the "Apply" button to enable the rule settings for this group. Click "Cancel" to undo the settings that have been entered.

After pressing the "Apply" button, a dialog box will pop up asking you if you would like to continue to add another group. Click "OK" to continue adding rules for another group, or click "Cancel" to return to the QnoKey Main Configuration Screen. As follows:



At this time QnoKey's Main Configuration screen will display the groups just being configured. This is shown in the figure below.

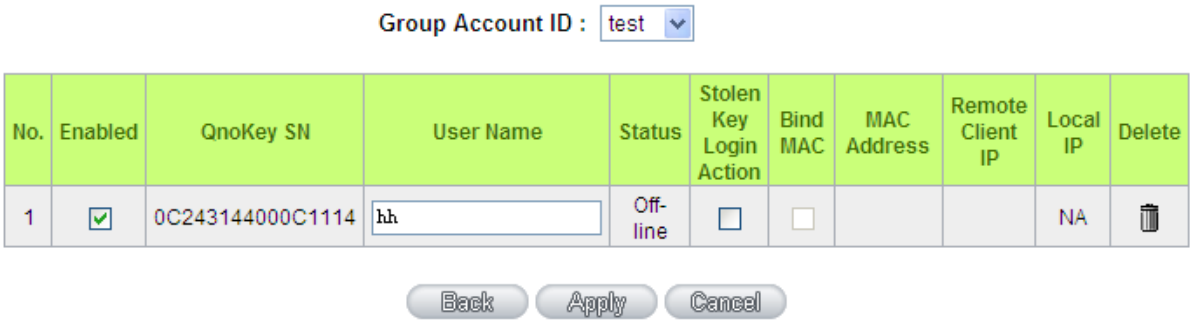


When new rules have been added, a "Show List" and an "Edit" button will appear after each of them. Click "Show List" to display the users of this group And click "Edit" to modify the settings. Click on the trash icon to delete thses rules.

4.3 Group Account List

Click on the "Show List" button to display the user data for the list of users in this group.

Group Account list



Group Account ID:	This shows this user's group name. You can select other groups by using the pull-down list.
Enabled:	Check this option to enable this QnoKey user.
QnoKey SN:	This displays the serial number for this QnoKey.
User Name:	This displays the user name for this QnoKey.
Status:	This displays the connection status for this QnoKey. "On-line" means that the user has established a connection successfully; "Off-line" indicates that there is no connection or connection is unsuccessful.
Stolen Key Login Action:	Once checked, QnoKey users will apply one of the protective actions.
Bind MAC:	If the "Bind MAC" option is selected, QnoKey can only be used on the computer with the MAC address it binds to. On a computer with a different MAC address, this QnoKey cannot be used.
MAC Address:	If the "Bind MAC" option is enabled, the MAC address that the QnoKey binds to will be displayed here. On a computer with a different MAC address, this QnoKey cannot be used.
Remote Client IP:	This shows the Public IP address that the QnoKey user uses to connect to the VPN remotely. If there is an NAT device in front of the remote QnoKey user's computer, then the IP address shown will usually be the WAN IP address of this device.
Local IP:	This shows the Private IP address used by the QnoKey user's computer to establish the remote connection. (If the remote computer is using a Public IP address to connect directly to the Internet, then this field will be the same as that of the Remote Client IP, and the remote user's Public IP address will be shown here.)

Delete:	Remove the QnoKey connectivity data for this particular user

V. Burning QnoKey--Writing Connectivity Data by Administrator

This section is mainly concerned with how to set PIN and write the data required for establishing IPSec VPN connection in a QnoKey. Before burning the QnoKey, you will need to install the QnoKey management software. The software can be installed from the CD-ROM. For installation instructions please refer to the installation procedures below.

5.1 Installing the QnoKey Management Software

There are two types of QnoKey installation softwares. One is the "QnoKey management software" used by the network administrator to burn the QnoKey and to write connection data to it; the other is the "QnoKey client software" intended for use by the ordinary user. When installing the "QnoKey management software," "QnoKey client software" will also be installed automatically." However, if only "QnoKey client software" is installed, "QnoKey management software" will NOT be installed along with it.

Place the QnoKey CD-ROM into your computer's optical drive. The disc will run automatically and display the following language selection screen. If the disc does not start automatically, run Untitled.exe file under the disc's directory.

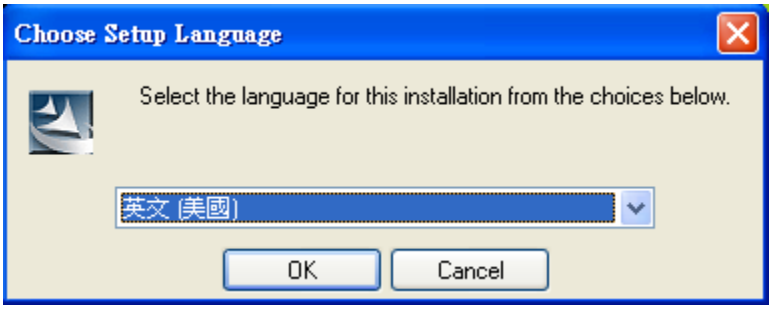
(1) Select "ENGLISH" and two options "QnoKey Management Software" and "QnoKey Client Software" will appear on the screen as follows.

(2) If you have Administrator privileges and would like to carry out the writing of connection data and burning of USB keys, please select "QnoKey Management Software." If you are an ordinary user, select "QnoKey Clinet Software" to install. The following will explain how USB Keys are burned, please install the "QnoKey management software" before proceeding.

※ Please note!

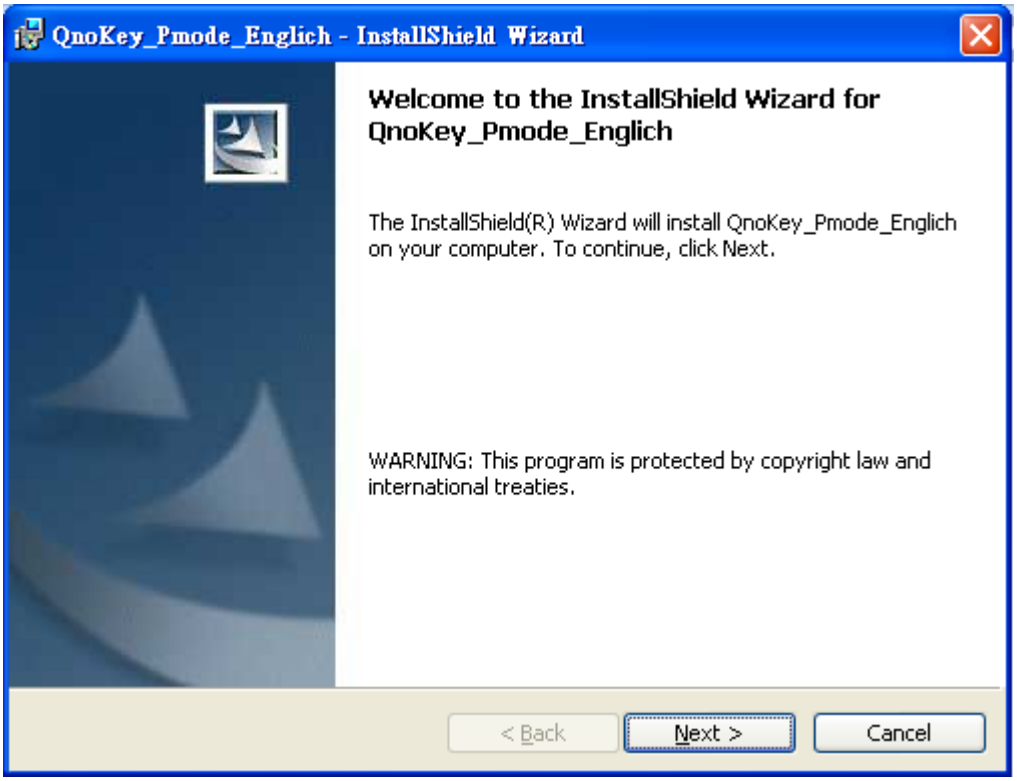
When installing "QnoKey Management Software," the "QnoKey Clinet Software" will also be installed automatically. However, if only "QnoKey Clinet Software" is installed, "QnoKey management software" will NOT be installed along with it.

(3) The "Choose Setup Language" dialog box will then appear, as shown in the figure below



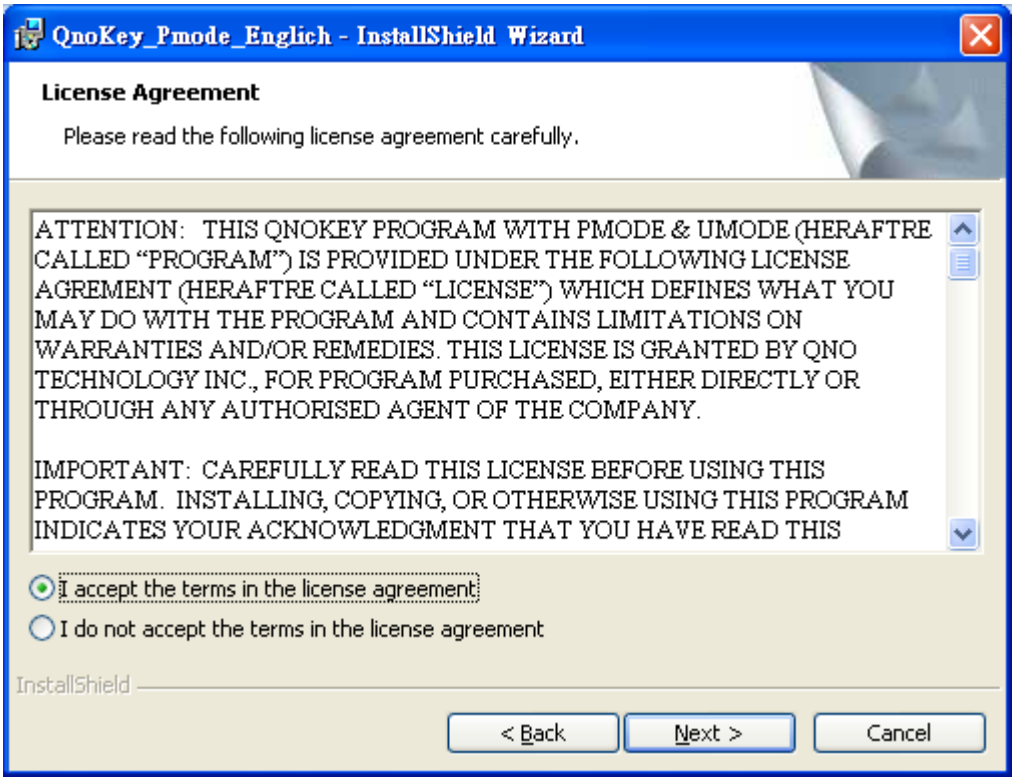
Please select English (US)

(4) After finishing checking the system's configuration, the setup program enters into the initial installation screen, as shown in the figure below



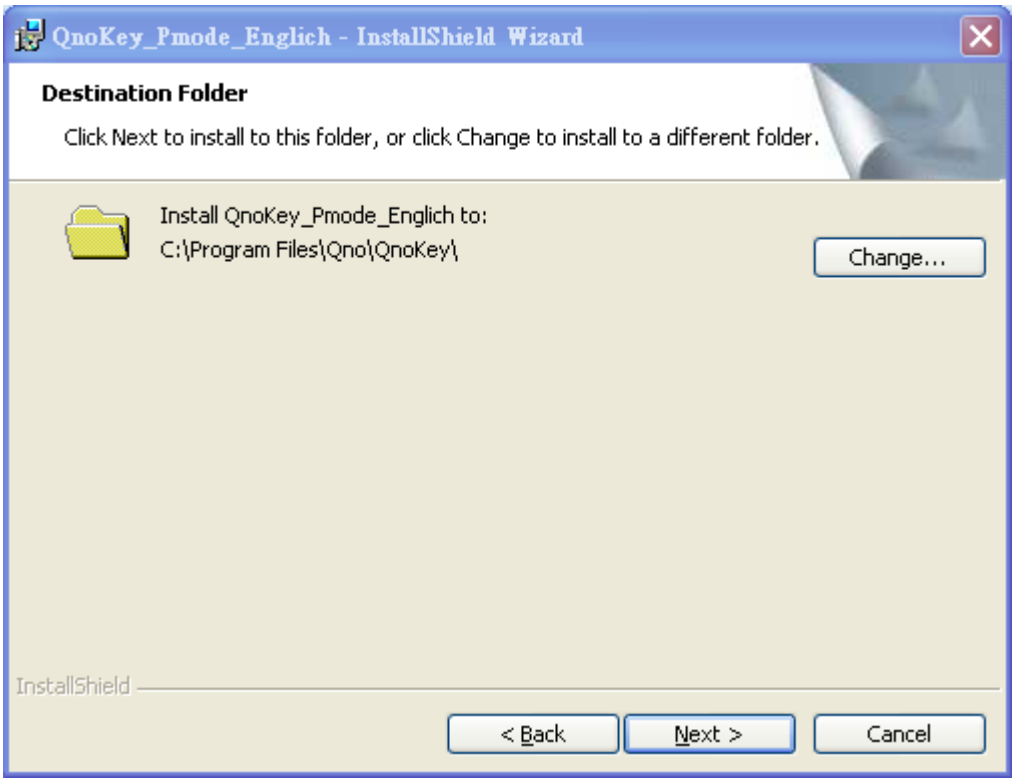
Please click "Next"

(5) The QnoKey software license agreement will appear. Please take your time to read it through carefully, and then click on the option "I accept the terms in the license agreement," as shown below



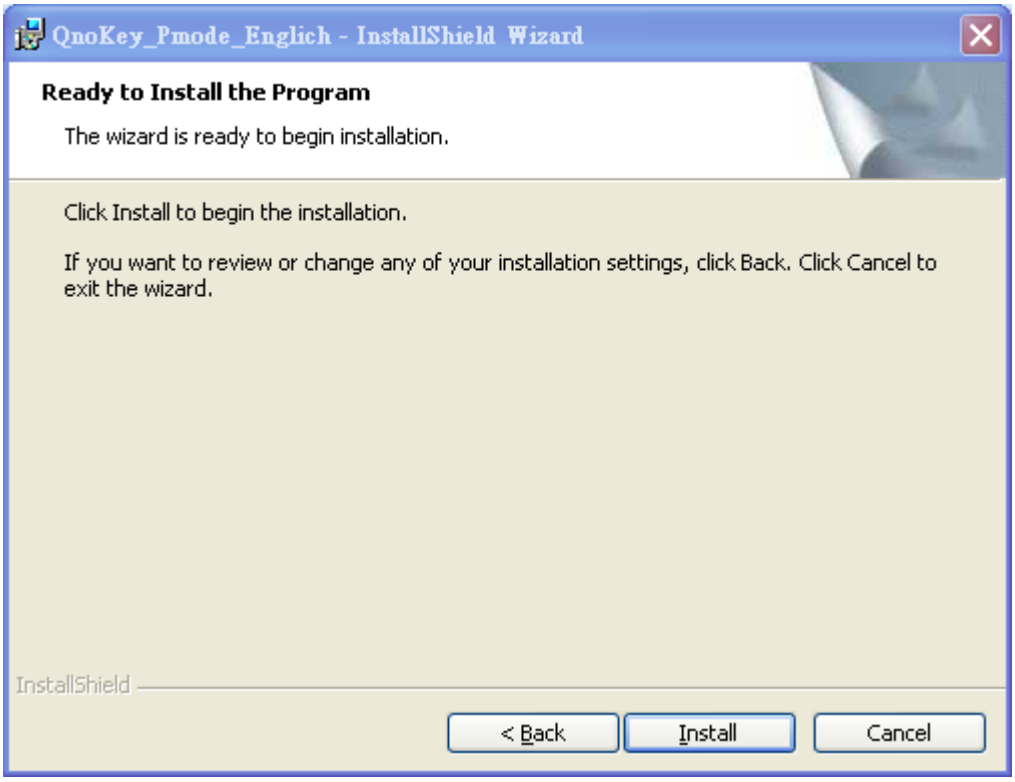
If you do not accept the terms of the agreement, you will not be able to continue the installation process

(6) Following you need to confirm the software installation folder. You can specify a different installation path by yourself; generally the default path will work

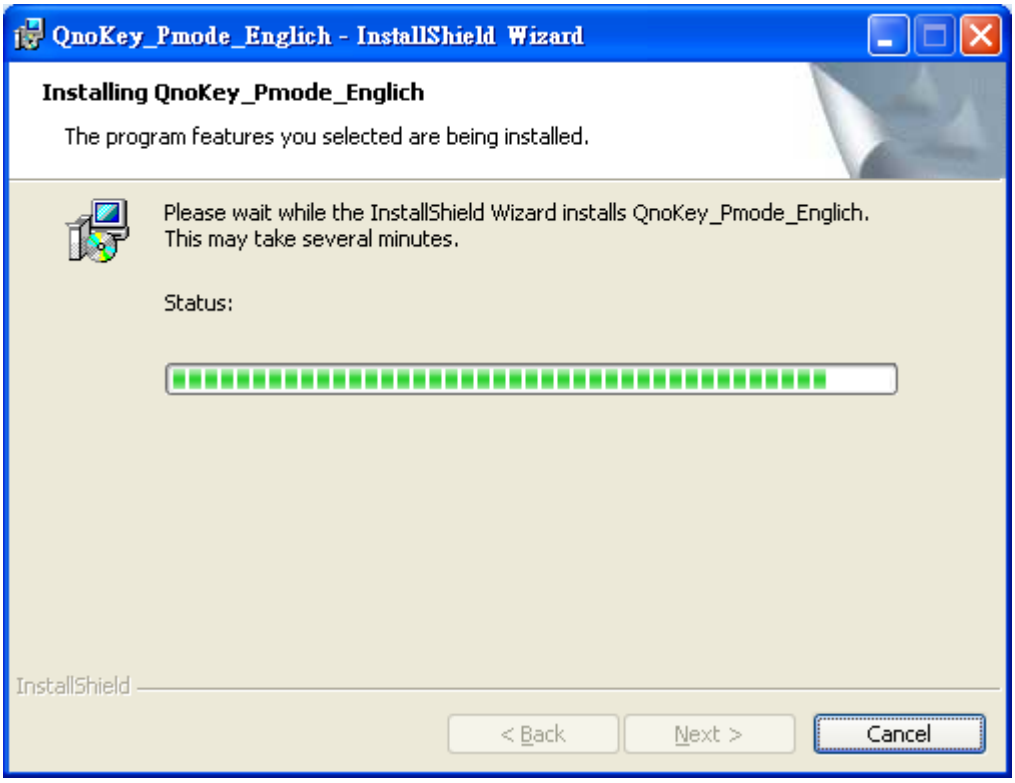


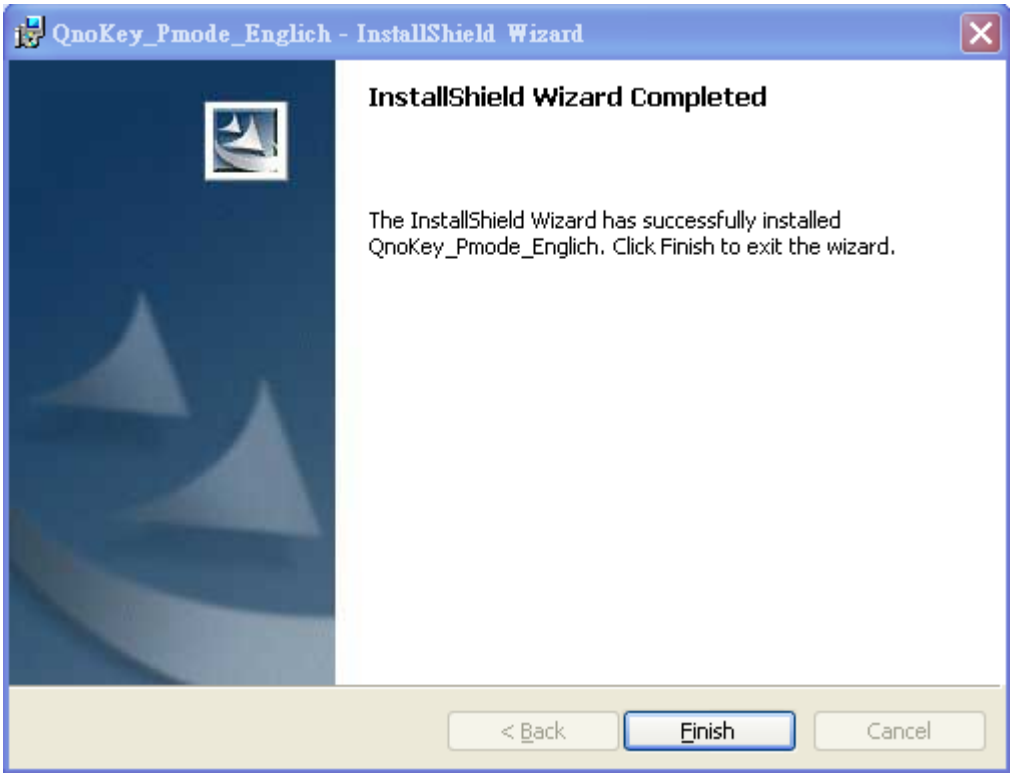
Click "Next" after confirmation

(7) Ready to install the program



(8)The following figures show the installation processes





Please press the "Finish" button to end the installation program. On the desktop, a QnoKey shortcut icon will appear, as shown in the following figure. It indicates that the management software has been successfully installed.

5.2 Run QnoKey Management Software to Burn USB Keys

Before running the QnoKey management program to burn data to a QnoKey, be sure to note the following:
(1) Ensure that you have already completed the initial configurations in QnoKey client-user (group settings).
(2) Please confirm that the QnoKey management software has been successfully installed on your computer.
(3) Make sure that the QnoKey has been inserted into the USB port.

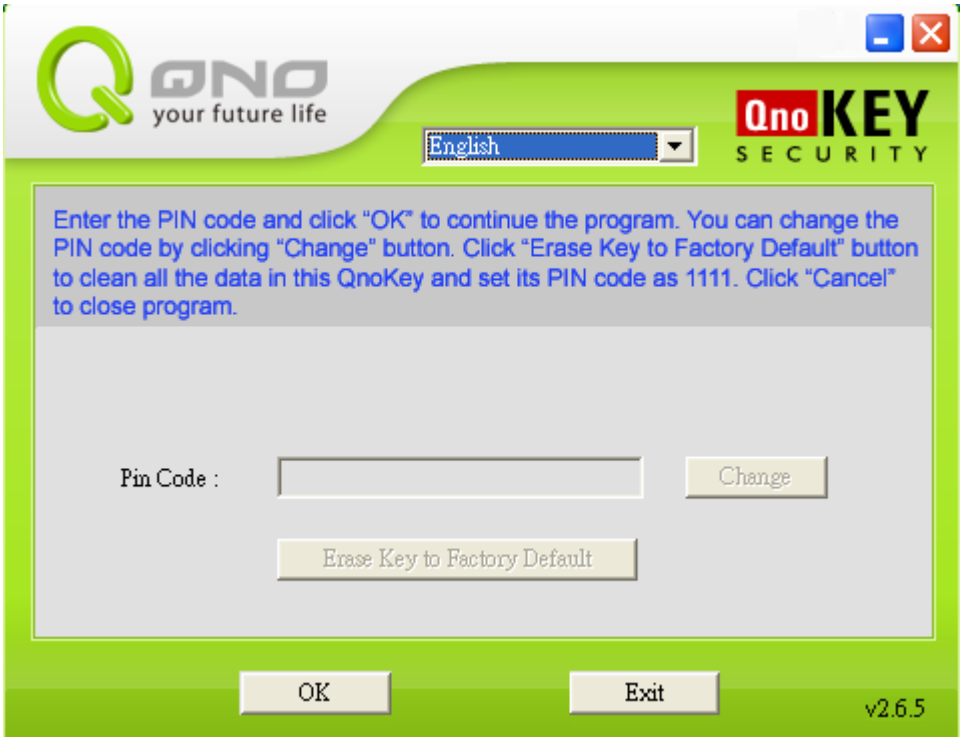
As the QnoKey administrator, before you proceed to burn a QnoKey, you need to obtain the administrator's account and password for the Qno router / firewall in order to be able to register the router in the QnoKey management program.

After you have confirmed the above, follow the procedures below to burn the QnoKey.

[1] Click on the QnoKey icon, as shown in the right of destop 

to bring up the QnoKey management program

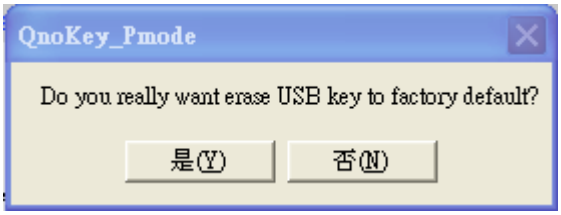
[2] The configuration page will appear firstly, as shown in the figure below. You may select the language at the top. Currently supported languages are: Simplified Chinese, Traditional Chinese and English. The information in the gray area provides step-by-step instructions on how the installation can be carried out.



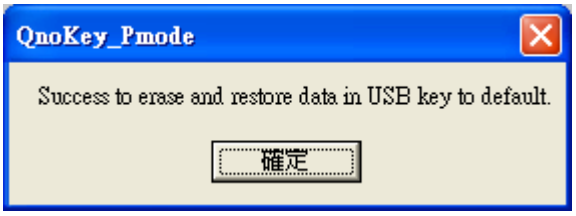
First, you need to enter the PIN code (personal identification code) in the password box. The factory default is 1111. If you wish to modify your PIN later, you can press the "Change" button and make the changes after you have entered both the old and new codes, as shown in the figure below

To confirm your new PIN, press the "Change" button and your new PIN will be saved and will take effect immediately. The following message box will pop up to indicate the success of the operation.

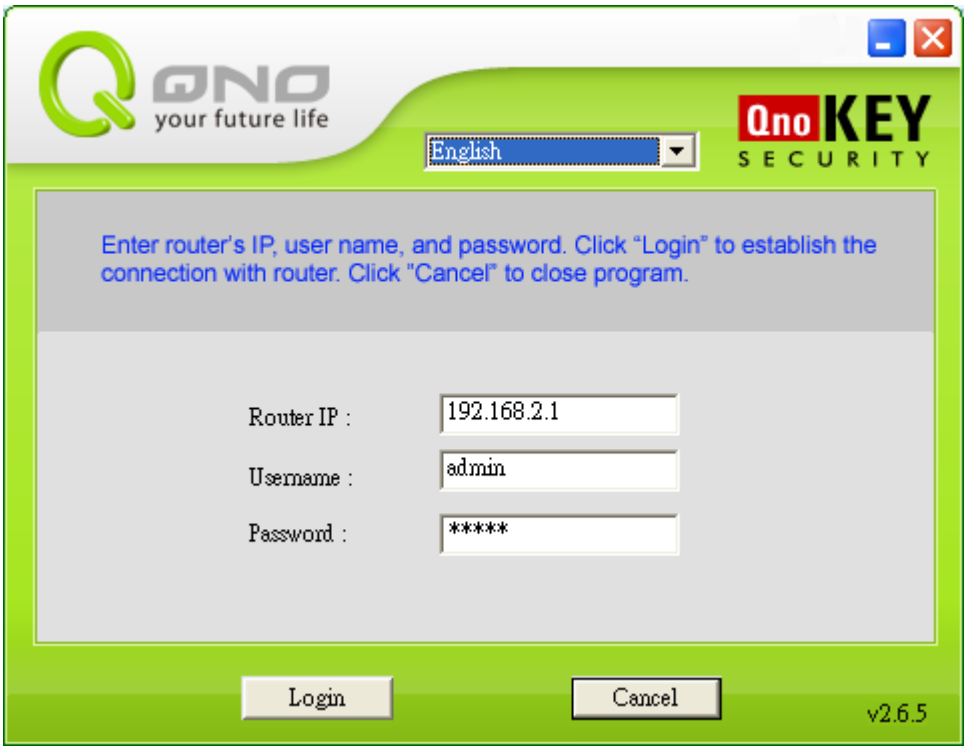
If you have forgotten the PIN code associated with this USB Key, you can press the "Erase Key to Factory Default" button. The management software will bring up a warning message box to confirm if you wish to erase all the data that has been burned into the QnoKey completely and the PIN code will be reverted to default.



Press "Yes" to erase all the data on the QnoKey and the PIN code will be reverted to the default settings, 1111, as shown in the figure below.

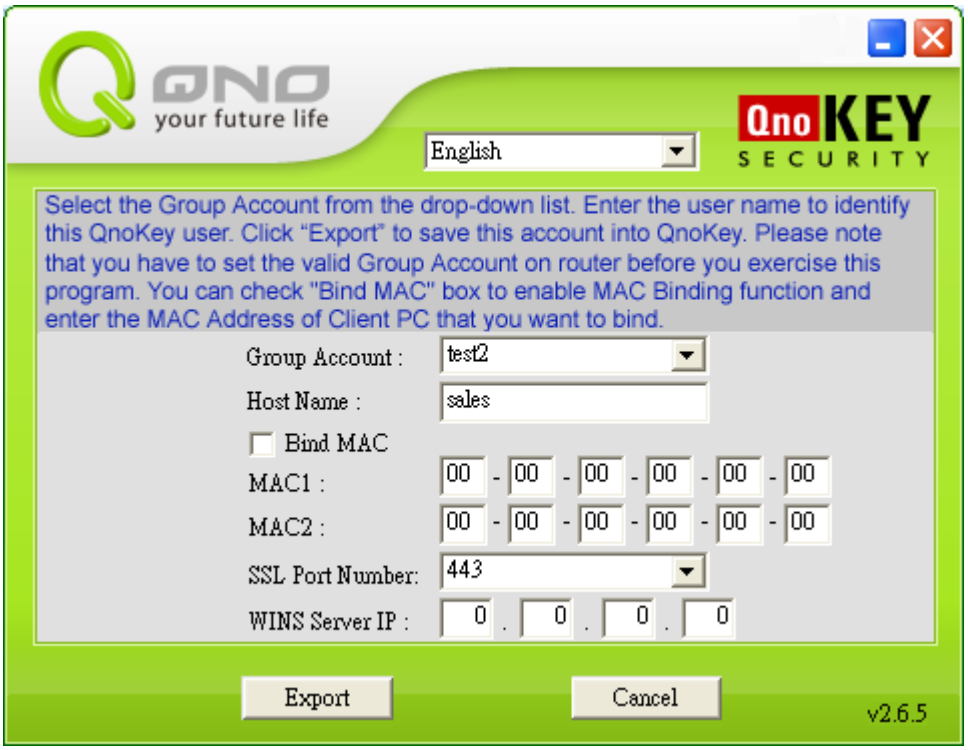


After you have entered the default PIN code 1111 and press OK, you must provide the following information into the corresponding fields: the Qno router / firewall IP address that has been configured in the QnoKey group account settings, administrator login ID and password, as indicated in the following figure.



※ **Please note!** What has been entered here is the WAN IP address of the router / firewall. Assuming there are several WAN ports and IP addresses in this router / firewall, then enter any of them, connection can be successfully established with the router / firewall and the burning operation for the QnoKey can be carried out, as long as the login ID and password are correct,

After successfully established a connection, the icon on the desktop's right corner will change from "disconnected"  to "connected"  (with the "tail" of the letter Q in the logo changing from gray to orange color), and the dialog box for burning connection data will be brought up, as shown in the figure below

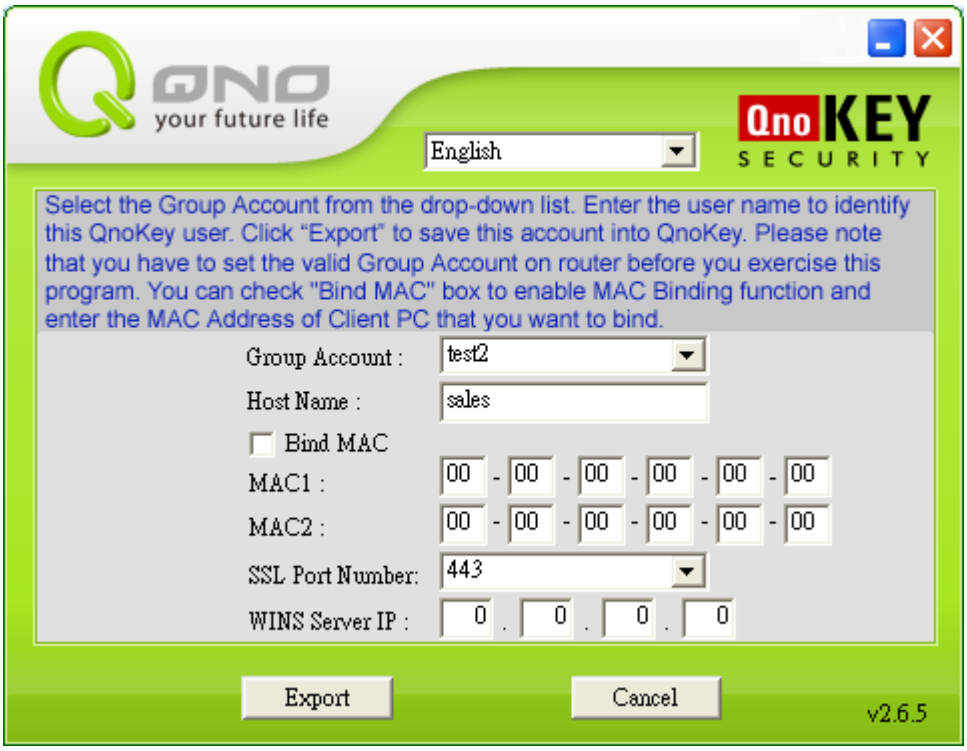


Group Account:	The pull-down menu is used to assign QnoKey and users to a specific QnoKey group. After it has been configured, the management settings and restrictions associated with the selected group will apply to the Key and to the users.
Host Name:	This identifies to whom the Key is assigned. For example, SalesWang
Bind MAC:	This specifies whether the Key will bind with the MAC address of the remote computer. If the option is not selected, MAC binding is disabled and the MAC address of the user's computer will not be checked. If you choose to enable it, you can enter two (at least one) MAC addresses. These will be checked against the MAC address of the user's computer when he/she attempts to establish a connection. If they do not

	match, connections will not be allowed.
MAC1 and MAC2:	After you have enabled "Bind MAC" ", enter the desired MAC address information for binding / checking.
SSL Port Number:	If ports 443 or 10443 have already been used by the Qno firewall / router itself to support other services (e.g. SSL VPN), it is recommended that you select a different port number for remote connection so as to avoid duplication. However, if connection is unsuccessful due to duplicated port numbers, QnoKey will still attempt to use a different port to establish an encrypted connection. Only when three attempts have been exhausted and a connection still cannot be made will the system display a "connection failure" status.
WINS Server IP:	If you have a WINS Server within the intranet served by the firewall / router, you can enter the server's IP address here. When the QnoKey user has successfully connected to the VPN, he/she may query and resolve the names of the computers/servers in the intranet via this WINS Server. If you do not need it, just enter enter0.0.0.0 in the IP address block.

Once the above configuration information has been correctly entered and confirmed, you can press the "Export" button to write these data to the QnoKey

After the data has been successfully exported, the above message box will appear. Press "Yes" to burn the data to another QnoKey that has not been burned with the same connection data. All fields will remain the same as the previous one, as shown in the figure below



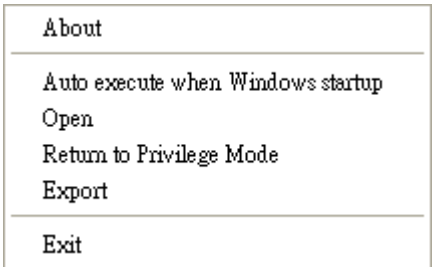
If part of this information needs to be modified for a different user's QnoKey, simply edit the information in the field(s), and there is no need to go through the same steps all over again. This feature can save the administrator a lot of time entering data from start to finish. It will reduce the time required to burn all the Keys significantly especially when there is a high demanding for QnoKey connection.

If you press "No", then the burning operation for this QnoKey is completed, and the management program as well as the burning process will automatically shut down.

※ **Please note!**

When management program is minimized, only the icon will remain on the system tray, as shown in the figure to the right 

At this time, if you right-click the Q-shaped icon, the following icon menu will appear:



※ About: This will display the software version of the QnoKey management program, as shown in the figure below.

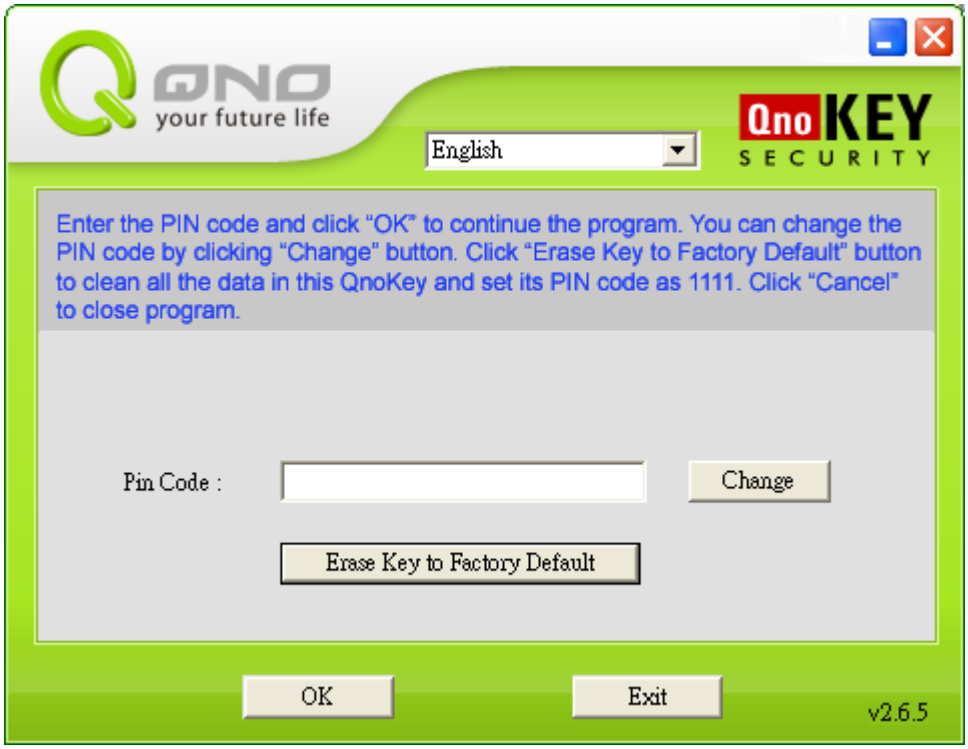
※ Auto execute when Windows starts up: If this option is checked, then next time the computer restarts, the QnoKey management program will be executed automatically

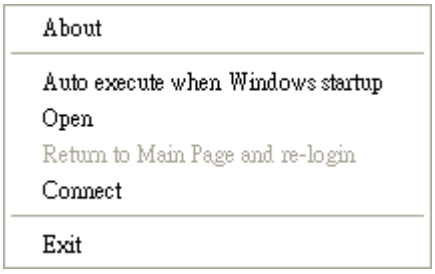
※ Open: Open and return to the original QnoKey management interface window

※ Return to Privileged Mode: Will return to the previous page of the QnoKey management interface window

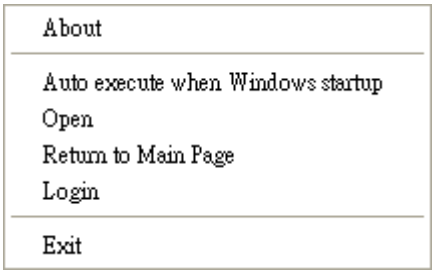
※ Export: Export IPSec VPN connection data to the QnoKey

※ **Please note!** The menu items available by right-clicking the Qno icon located at the lower right corner will change as the main interface window changes, but essentially associated with what can be performed on the main window. Refer to the following figure for the exact correspondence:

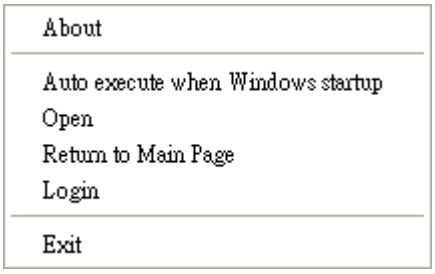

your future life
English
Qno KEY
SECURITY
Enter the PIN code and click "OK" to continue the program. You can change the PIN code by clicking "Change" button. Click "Erase Key to Factory Default" button to clean all the data in this QnoKey and set its PIN code as 1111. Click "Cancel" to close program.
Pin Code :
Change
Erase Key to Factory Default
OK
Exit
v2.6.5

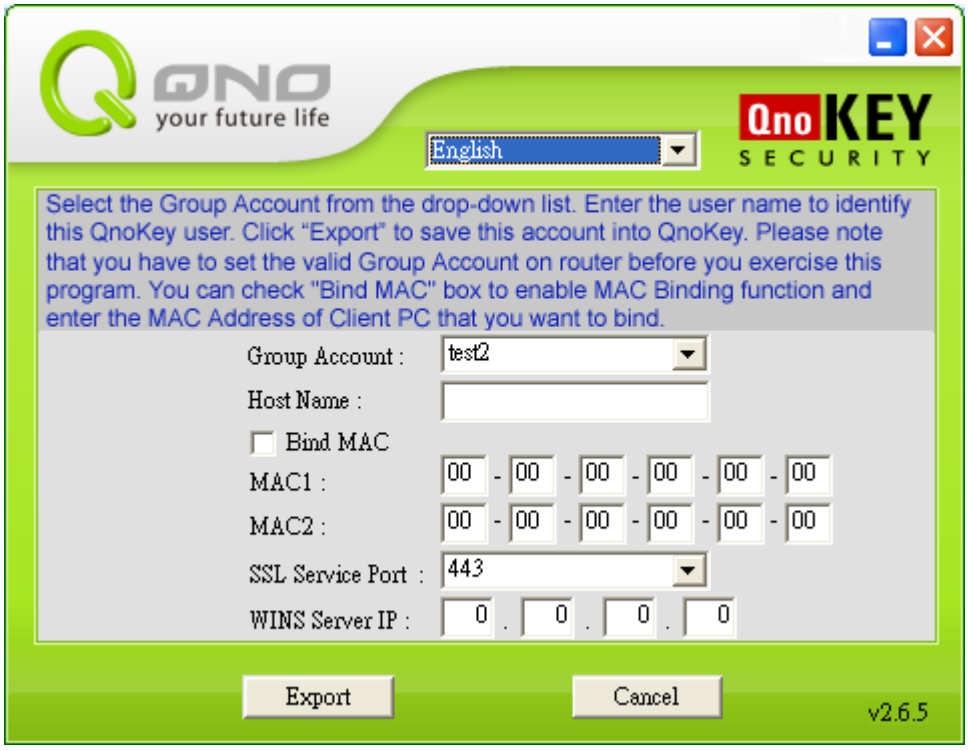

About
Auto execute when Windows startup
Open
Return to Main Page and re-login
Connect
Exit

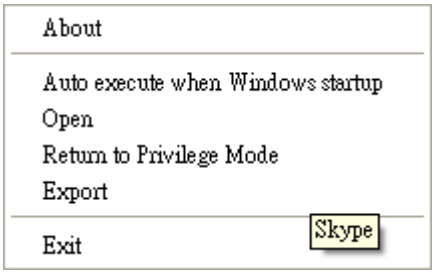

your future life
English
Qno KEY
SECURITY
Enter current password in "Old Password" column. Enter the new password you wish to use in "New Password Column". Enter the new password again in "Confirm New Password" column. Please note that the password can be alphanumeric and special characters. The maximum length is 15 characters.
Old Pin Code :
New Pin Code :
Confirm New Pin Code :
Change
Cancel
v2.6.5


About
Auto execute when Windows startup
Open
Return to Main Page
Login
Exit


your future life
English
QnoKEY
SECURITY
Enter router's IP, user name, and password. Click "Login" to establish the connection with router. Click "Cancel" to close program.
Router IP :
Username :
Password :
Login
Cancel
v2.6.5


About
Auto execute when Windows startup
Open
Return to Main Page
Login
Exit


your future life
English
QnoKEY
SECURITY
Select the Group Account from the drop-down list. Enter the user name to identify this QnoKey user. Click "Export" to save this account into QnoKey. Please note that you have to set the valid Group Account on router before you exercise this program. You can check "Bind MAC" box to enable MAC Binding function and enter the MAC Address of Client PC that you want to bind.
Group Account : test2
Host Name :
Bind MAC
MAC1 : 00 - 00 - 00 - 00 - 00 - 00
MAC2 : 00 - 00 - 00 - 00 - 00 - 00
SSL Service Port : 443
WINS Server IP : 0 . 0 . 0 . 0
Export
Cancel
v2.6.5


About
Auto execute when Windows startup
Open
Return to Privilege Mode
Export
Exit
Skype

VI. QnoKey User Connection Mode

This chapter focuses on how the general user can gain access to the VPN using the provided connection software and the QnoKey obtained from the network administrator. Before making a VPN connection, you need to install the QnoKey client software first. If the network administrator has already installed the software for you, you can simply run the QnoKey client connection program. This program can also be installed from the CD-ROM. If you need to install it yourself, please refer to previous section on the installation of the software via CD-ROM (Sec. 5.1), and choose to install only the "QnoKey Client Software." There is no need to install the management software (since the ordinary user will not need to run the QnoKey management software).

6.1 Running the QnoKey User Connection Program

After the QnoKey Client Software has been installed, the QnoKey icon will appear on your computer's desktop, as shown in the figure to the right. 

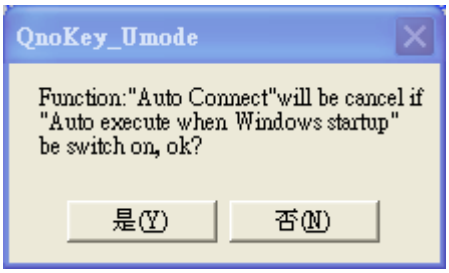
To establish a connection via QnoKey, please click on the icon to run the program. The following main connection window will appear.

You may select the language at the top of the page. Currently supported languages are: Simplified Chinese, Traditional Chinese and English. The information in the gray area provides step-by-step

instructions on how the installation can be carried out.

For password, please enter the PIN code (personal identification code) obtained from the network administrator along with the QnoKey intended for the ordinary user.

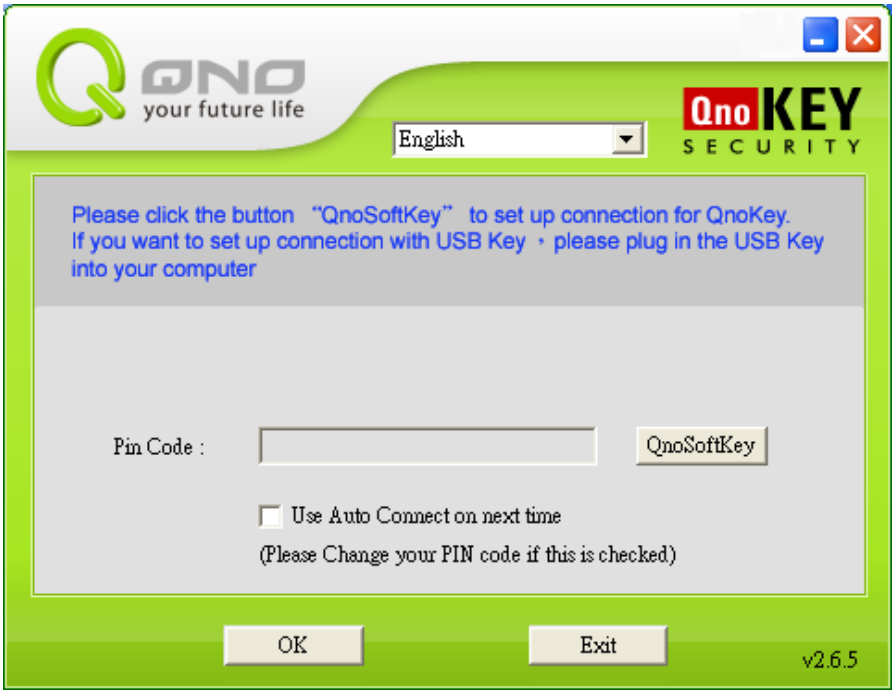
The option "Use Auto Connect next time" allows you to simplify the steps of starting the program and entering the PIN code. If this feature is enabled, the user connection program will start itself the next time you insert the USB Key. The QnoKey connection process will be carried out automatically and there is no need to enter the password. After the option has been checked, the system will ask the user to confirm the activation of "Auto Connect", and proceed to disable the "Auto execute when Windows starts up" function. (Note)



Selecting "Yes" will cause the following warning message box to pop up, which indicates that this feature will take effect only after the system restart. In another word, before the next reboot, unplugging the USB Key and re-inserting it will not perform an auto connect.

※ Note:

Only one of "Auto execute when Windows startup" and "Auto Connect" can be enabled at a time. If "Auto execute" is enabled, the QnoKey connection program will be automatically run and the user needs to manually enter the PIN code on the connection dialog, as shown in the figure below.



When the computer is on, as soon as the QnoKey is inserted into the computer, connection with the VPN will be attempted automatically. When a connection is attempted for the first time and the PIN code is entered and confirmed, QnoKey's "Q" icon located at the lower right corner of the system tray will begin the connection. For subsequent connections, the main dialog box for PIN code will no longer pop up, unless the user specifically moves the mouse cursor to the "Q" icon, right-clicks on it, and selects "Open" from the menu, the connection dialog box will not appear at all.

After entering the correct PIN code (personal identification code), the dialog box that displays the connection messages will appear, as follows

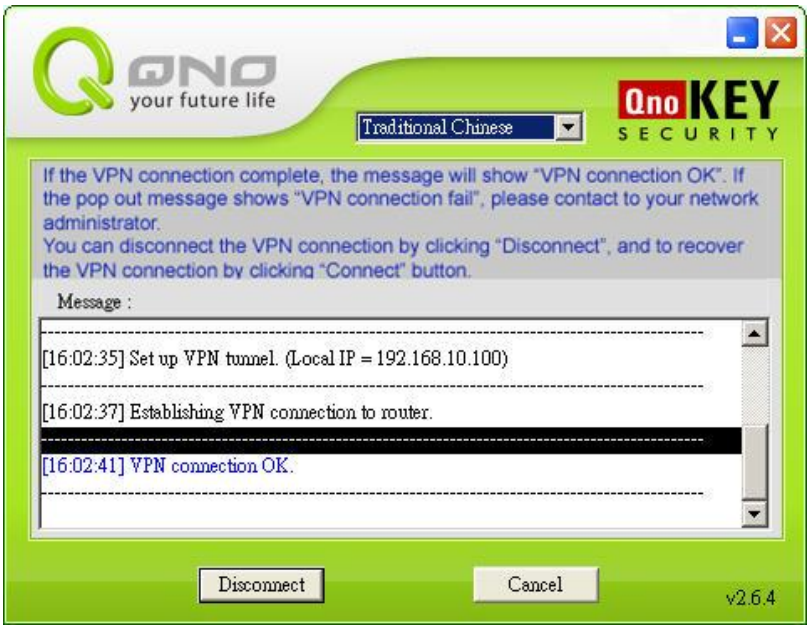
Press the "Connect" button to establish a VPN connection. Press "Cancel" to return to the previous page for entering PIN code

Press the "Connect" button at this time. The QnoKey connection program will attempt to establish a connection using the data that has been burned onto the QnoKey by the network administrator.

Refer to the following table for messages that will appear during the connection process:

Start connection and challenge response protocol
Get challenge from router
Send response to router
Got preshared key and IPSec SA data
Set up VPN tunnel
Establishing VPN connection to router
VPN connecttion OK

If the connection with the VPN is established successfully, the message "VPN Connection OK" will appear in the window, as shown in the following diagram

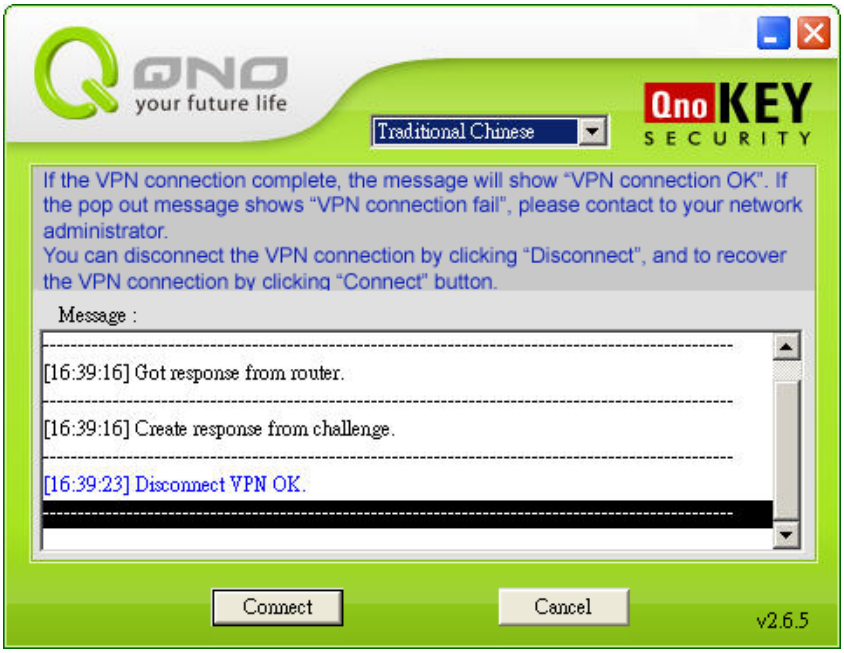


A call-out message box with the text "Status: Connected" will also appear at the lower right corner of the system tray where the Q icon is located, and the tail of the letter Q will turn orange.

If there is a problem during the process and a connection cannot be established, please record the text of the connection messages and send it to the agent, distributor, or the manufacturer's technical support staff for consultation.

6.2 Terminating VPN Connections

When there is no further need to connect to the VPN, you can press "Disconnect" to terminate the VPN connection in order to safeguard your data. When the connection is terminated, the message "Disconnect VPN OK" will appear, as shown in the figure below.



A call-out message box with the text "Status: Disconnected" will also appear at the lower right corner of the system tray where the Q icon is located, and the tail of the letter Q will turn gray, as shown in the figure to the right. 

When the VPN has been terminated, for security purposes you can unplug the QnoKey and keep it in a safe location. If the QnoKey is removed when the computer is still connected to the VPN, the user connection program will terminate by itself. The established IPSec VPN tunnel will also be removed.

Appendix I: Commonly encountered problems and suggestions when using QnoKey

Question 1: I've set up QnoKey function on the router and burned the data onto the QnoKey. Why my user program still shows a failed VPN connection?

Answer: Check the client computer to see if the Windows Operating System used is XP, 2000, Vista or Win 7; Also check to make sure whether the network is disconnected, congested due to heavy traffic, or connections being blocked by the firewall. If the above checks reveal no abnormal situations, please reinstall the QnoKey Client Software on the user's computer.

Check to see if the WAN IP entered into the router is correct. Make sure the corresponding fixed WAN IP is correct, and if there is no fixed IP, fill in the correct domain name. If there is no WAN to be connected, leave the field blank. Re-export the data to the QnoKey, and attempt to re-connect to the VPN on the client side.

Question 2: If I lose the QnoKey by accident, what should I do to safeguard information security on the VPN?

Answer: First of all, identify the group account of the lost QnoKey. Then reconfigure this group account in the router's management UI, choose "Prohibit connection" in the "Stolen Key Login Action" option to in order to prevent the QnoKey that has been lost from making VPN connections, thus ensuring data security on the network.

Question 3: In user mode, why there is no VPN connection after I enter the password?

Answer: After you have entered your password, the page that allows you to perform the connection action will then be shown. Click on the "Connection" button at the lower left corner to begin VPN connection. At this time, messages sent back and forth by the server and client sides will be displayed in the message field.

Question 4: After the life time configured on a QnoKey has expired, can I continue to use it?

Answer: When the QnoKey's life time has expired, you won't be able to make VPN connections, but a new QnoKey can be created. If other settings are unchanged, you can carry out the steps directly to create a new QnoKey. If there are modifications, new configuration steps need to be performed, and the new data will overwrite the original content.

Appendix II：Qno Technical Support Information

For more information about Qno's product and technology, please log into Qno's bandwidth forum, refer to the examples of the FTP server, or contact the technical department of Qno's dealers as well as the Qno's Mainland technical center.

Qno Official Website

http：//www.Qno.com.tw

Dealer Contact

Users may log on to the service webpage to check the contacts of dealers.

http：//www.qno.com.tw/web/where_buy.asp

Taiwan Support Center：

E- mail：QnoFAE@qno.com.tw