

IPSec VPN Remote Client

Setup Guide For Wiws XP and Vista



Table of Contents

1.	Introduction	3
2.	How to install VPN Client Software	4
3	How to configure / use VPN Client	9



1. Introduction

HKBN's IP-VPN Service allows mobile or remote users to access the corporate network with the highest level of security through the Internet.

After installation of the IPSec VPN Remote Client software, transmission of data between the remote users and the corporate MPLS IP-VPN network is protected by encryption and authentication.

This user guide will direct you step-by-step to install the software and enable remote access.

Before you start to access the corporate network, you are recommended to have the following prerequisite information:

1. Group Access Information

2. Your login username and password



2. ow to install VPN Client Software

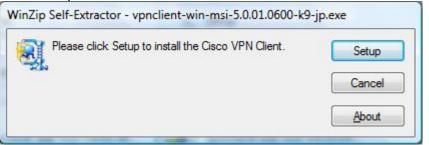
For Windows XP and Vista 32bit/ 32bit SP1

Please make sure that you are installing the IPSec Remote Client software for your Windows XP or Vista platform.

We use "Cisco System VPN Client 5.0" in this user guide.

Installation Steps:

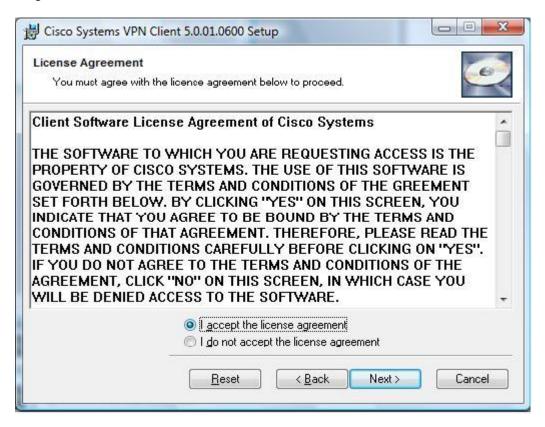
- a) Double click to extract the file.
- b) Click "setup".



c) "Welcome" message will pop-up. Click "Next" to continue.

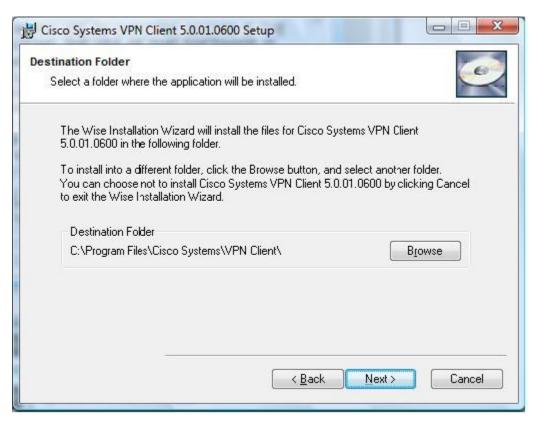


d) "License Agreement" will pop up. (Please read it carefully.) Select "I accept the license agreement" and click "Next" to continue.



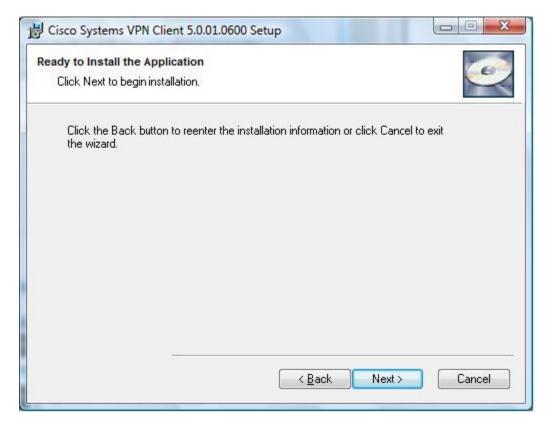


e) "Destination Folder" will pop up. Click "Browse" to install the software at your Destination Folder or click "Next" to install at default folder.



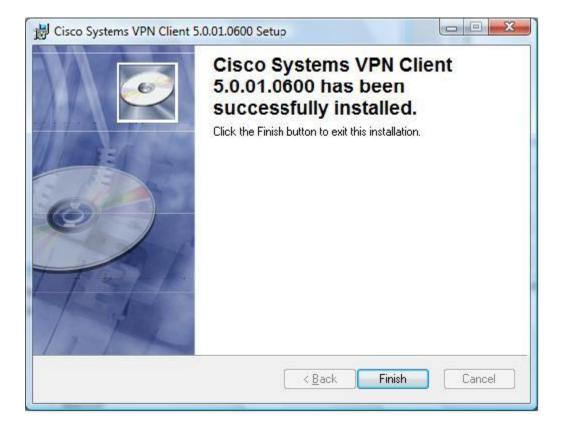


f) Click "Next" to start Installation.

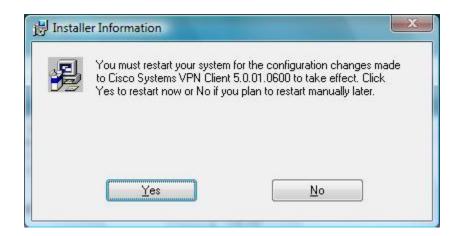




g) Click "Finish" to exit the installation.



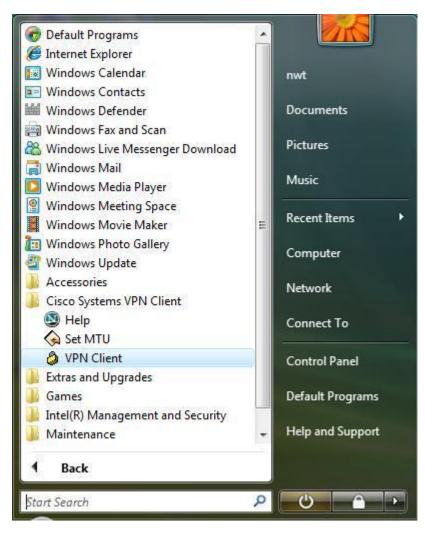
h) Click "Yes" to Reboot.





3 How to configure / use VPN Client

1. After installation, select "VPN Dialer" from the "Programs Menu".





2. Click "New" to create a new profile for the VPN connection.

status: Disconnected VPN Client - Version 5.0.01.0600		
onnection Entries <u>S</u> tatus C <u>e</u> rtificates <u>L</u> og <u>O</u> ptions <u>H</u>	lelp	
Connect New Import Modify Delete	9	cisco
Connection Entries Certificates Log		
Connection Entry	Host	Transport



 Enter the name of the connection in the field "Connection Entry", e.g. "Main Office". Enter the IP address of the VPN Concentrator in the field "Host", e.g. "203.98.128.213". Enter the Group Access Information in the field "Group Name and Group Key". Then click "Save".

Connection Entry: Ma	ain Office			ahah cisco		
	3.98.128.21: iransport	3 Backup Servers	Dial-Up			
	ation		C Mutual Gro	up Authenticatio	on	
Name:	iv 1234567	78_ra_groupname				Group Nam
Password:					-	Group Key
Confirm Password	l: 					
C Certificate Authe	ntication					
Name:		<u></u>				
Send CA Cert	ificate Chain					



4. Highlight the Entry just created and click "Connect" to start the VPN connection.

Status: Disconnected VPN Client - Version 5.0.01.0600		
<u>Connection Entries</u> <u>Status</u> C <u>e</u> rtificates <u>Log</u> Options <u>H</u> e	lp	
Connect New Import Modify Delete		cisco
Connection Entries Certificates Log	T	
Connection Entry	Host	Transport
Main Office	203.98.128.213	IPSec/UDP
4		
Not connected.		

5. A window will pop up. Please enter the "Username" and "Password".

	sted the followi	ng information to complete	e the user
authentication.			
	demo@gigali	nkvpn.com	
CISCO Password:			
Lassword.	1		-11.7
		OK	Cancel



 After connecting to the VPN, a VPN Client icon will appear at the System Tray (Lower Right corner of the Desktop). User may disconnect the VPN by right-clicking the icon and selecting "Disconnect".

Log Window
Notifications
Disconnect
 About VPN Client
 🖢 🔄 💽 📢 📢 📢 10:51 AM

7. More information will be displayed by right clicking the icon in the System Tray and choosing "Statistics".

Contraction of the second		
Statistics		
Log Window		
Notifications		
Disconnect		
About VPN Client		
2 🔄 🛇 📑 🤫 📑 🖓 10:51 A	M	
PN Client Statistics		
	I	
nnel Details Route Details	Firewall	
Address Information	Connection Information	tion
Client: 10.10.200.2	Entry:	Main Office
Server: 203.98.128.213	Time:	0 day(s), 00:02.22
	Crypto	
Bytes		
Bytes Received: 0		56-bit DES
	Encryption: Authentication:	56-bit DES HMAC-MD5
Received: 0 Sent: 0	Encryption: Authentication:	
Received: 0 Sent: 0	Encryption: Authentication: Transport	HMAC-MD5
Received: 0 Sent: 0 Packets	Encryption: Authentication: Transport	HMAC-MD5
Received: 0 Sent: 0 Packets Encrypted: 0	Encryption: Authentication: Transport Transparent Tunne	HMAC-MD5 ling: Active on UDP port 4500
Received: 0 Sent: 0 Packets Encrypted: 0 Decrypted: 0	Encryption: Authentication: Transport Transparent Tunne Local LAN:	HMAC-MD5 ling: Active on UDP port 4500 Disabled
Received: 0 Sent: 0 Packets Encrypted: 0 Decrypted: 0 Discarded: 3	Encryption: Authentication: Transport Transparent Tunne Local LAN:	HMAC-MD5 ling: Active on UDP port 4500 Disabled
Received: 0 Sent: 0 Packets Encrypted: 0 Decrypted: 0 Discarded: 3	Encryption: Authentication: Transport Transparent Tunne Local LAN:	HMAC-MD5 ling: Active on UDP port 4500 Disabled None
Received: 0 Sent: 0 Packets Encrypted: 0 Decrypted: 0 Discarded: 3	Encryption: Authentication: Transport Transparent Tunne Local LAN:	HMAC-MD5 ling: Active on UDP port 4500 Disabled None