

UNIOTP BUILDING VPN MANUAL

VERSION 1.1

SecuTech

www.eSecuTech.com

The data and information contained in this document cannot be altered without the express written permission of SecuTech Solution Inc. No part of this document can be reproduced or transmitted for any purpose whatsoever, either by electronic or mechanical means.

The general terms of trade of SecuTech Solution Inc. apply. Diverging agreements must be made in writing.

Copyright © SecuTech Solution Inc. All rights reserved.

WINDOWS is a registered trademark of Microsoft Corporation.

The WINDOWS-logo is a registered trademark ^(TM) of Microsoft Corporation.

Software License

The software and the enclosed documentation are copyright-protected. By installing the software, you agree to the conditions of the licensing agreement.

Licensing Agreement

SecuTech Solution Inc. (SecuTech for short) gives the buyer the simple, exclusive and non-transferable licensing right to use the software on one individual computer or networked computer system (LAN). Copying and any other form of reproduction of the software in full or in part as well as mixing and linking it with others is prohibited. The buyer is authorized to make one single copy of the software as backup. SecuTech reserves the right to change or improve the software without notice or to replace it with a new development. SecuTech is not obliged to inform the buyer of changes, improvements or new developments or to make these available to him. A legally binding promise of certain qualities is not given. SecuTech is not responsible for damage unless it is the result of deliberate action or negligence on the part of SecuTech or its aids and assistants. SecuTech accepts no responsibility of any kind for indirect, accompanying or subsequent damage.

Contact Information

HTTP: www.eSecuTech.com

E-Mail: Sales@eSecuTech.com

Please Email any comments, suggestions or questions regarding this document or our products to us at: Sales@eSecuTech.com

Version	Date
1.0	2011.4.21
1.1	2012.4.4

CE Attestation of Conformity



UniOTP is in conformity with the protection requirements of CE Directives 89/336/EEC Amending Directive 92/31/EEC. UniOTP satisfies the limits and verifying methods: EN55022/CISPR 22 Class B, EN55024: 1998.

FCC Standard



This device is in conformance with Part 15 of the FCC Rules and Regulation for Information Technology Equipment.

Operation of this product is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Conformity to ISO 9001:2000



The Quality System of SecuTech Solution Inc., including its implementation, meets the requirements of the standard ISO 9001:2000

ROHS



All UniOTP products are environmental friendly with ROHS certificates.

Table of Contents

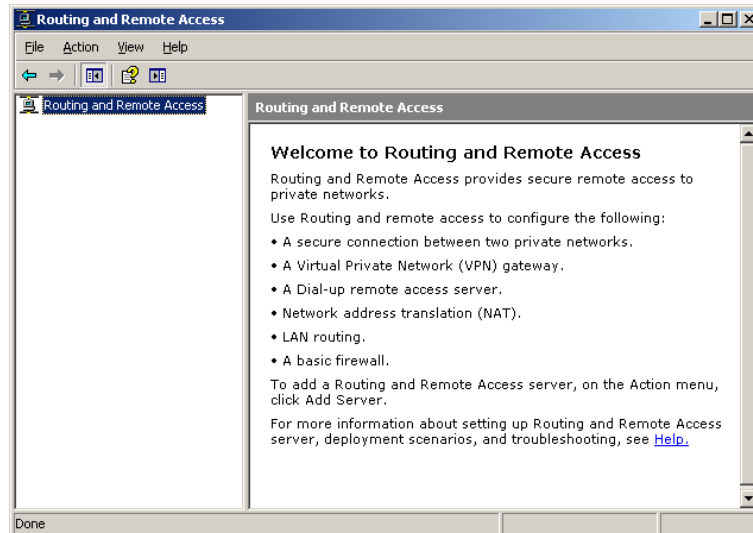
ABOUT THIS GUIDE	1
CHAPTER 1: ROUTING & REMOTE ACCESS	2
CHAPTER 2: ENVIRONMENT CONFIGURATION.....	5
CHAPTER 3: VPN SERVER WITH UNIOTP	6
CHAPTER 4: ADD VPN CLIENT	11
CHAPTER 5: APPENDIX:.....	18
5.1 Common errors in VPN clients connect to server:	18

About this guide

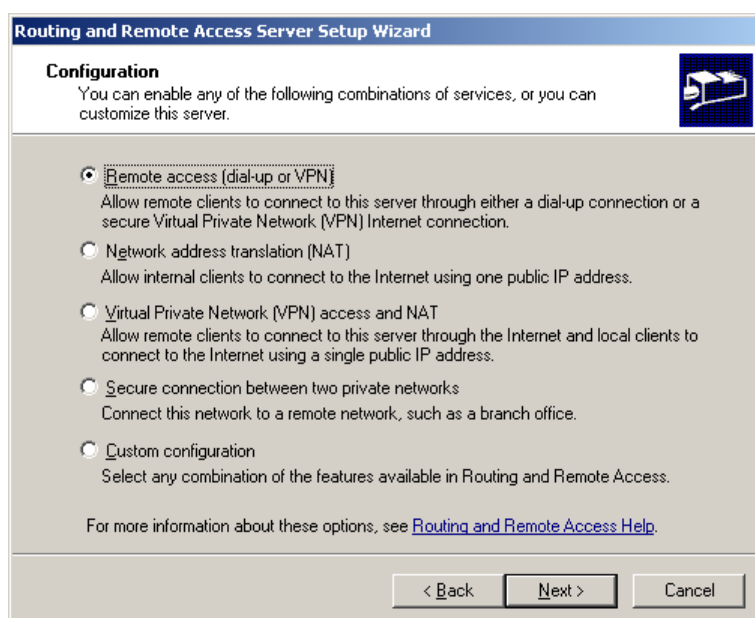
VPN (Virtual Private Network) refers to two different equipment (a computer and firewall) with VPN link capability which can form a secure tunnel over the internet. In the tunnel initiator (server), A user's private data is encapsulated and encrypted, and then transmitted on the internet; in the receiver side (client), the received data is unpacked and decrypted. VPN services are installed with Windows 2000/2003. This manual is based on the installed VPN service, named Routing and Remote Access. You can find this service from Start→Program→Administrative Tools→Service.

Chapter 1: Routing & Remote Access

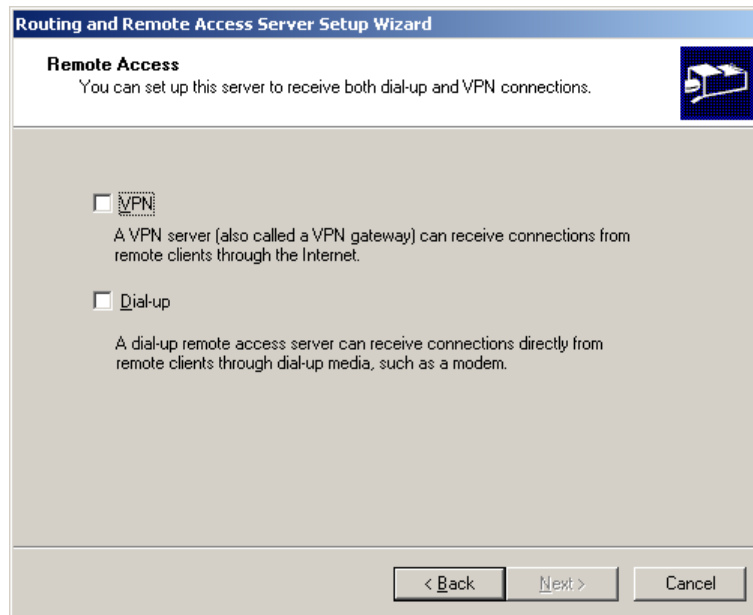
From Start→Program→Administrative Tools→Routing and Remote Access, please open the Routing and Remote Access panel. Right-Click on “Routing and Remote Access” on the left-side of the panel, please select “add server” to add a VPN server.



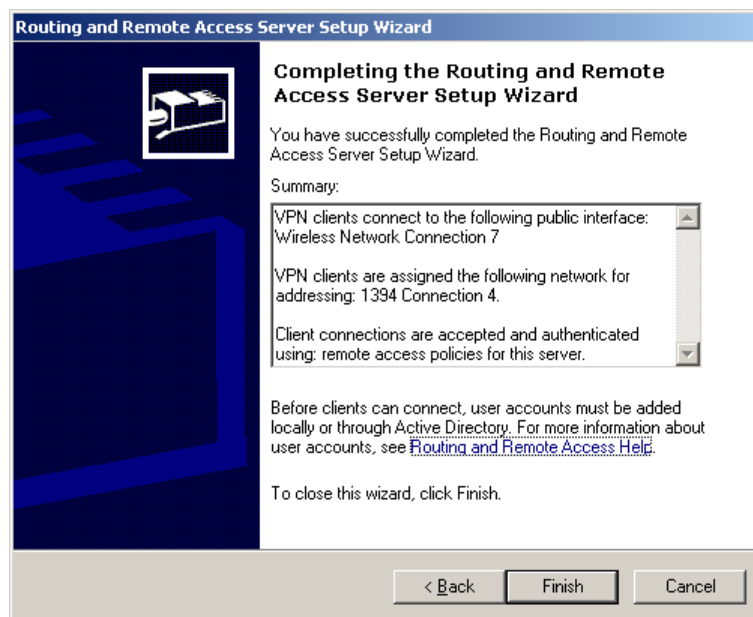
Right click on the added server, and select “Configure and Enable Routing and Remote Access”. If the Windows Firewall/Internet Connection Sharing (ICS) service is enabled, the Routing and Remote Access service cannot be enabled, and an ICS service warning message will appear. Disable the ICS service and redo the above operation. After turning on Routing and Remote Access, the following configuration wizard will appear.



Select Remote access (dial-up or VPN) and click next to get into the next page.

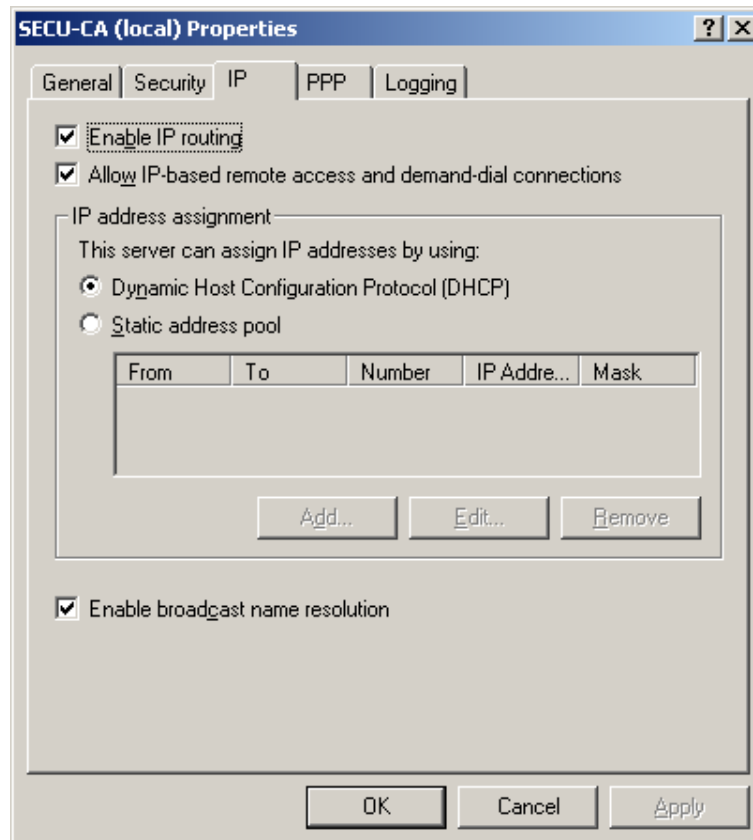


Finish VPN installation. The next step is configuration.



Chapter 2: Environment configuration

Right-click on the directory tree in the server name, select property and switch to the IP address tab.

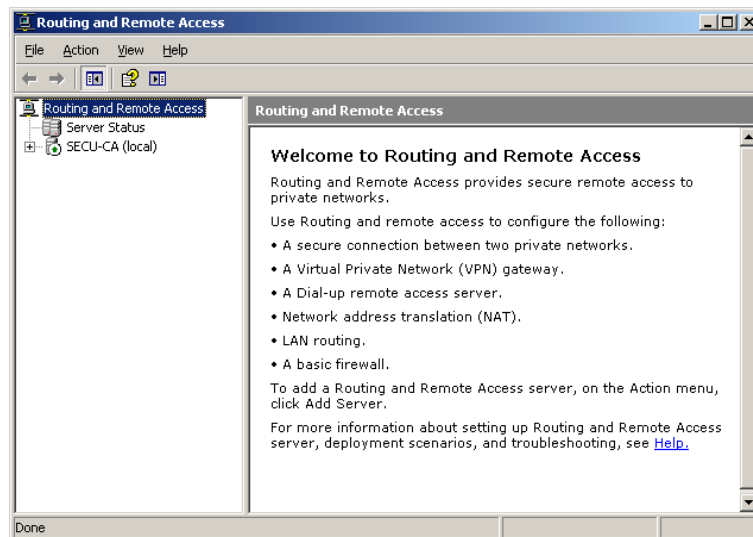


Using a static address pool will reduce the time to resolve an IP address, and will increase network speed

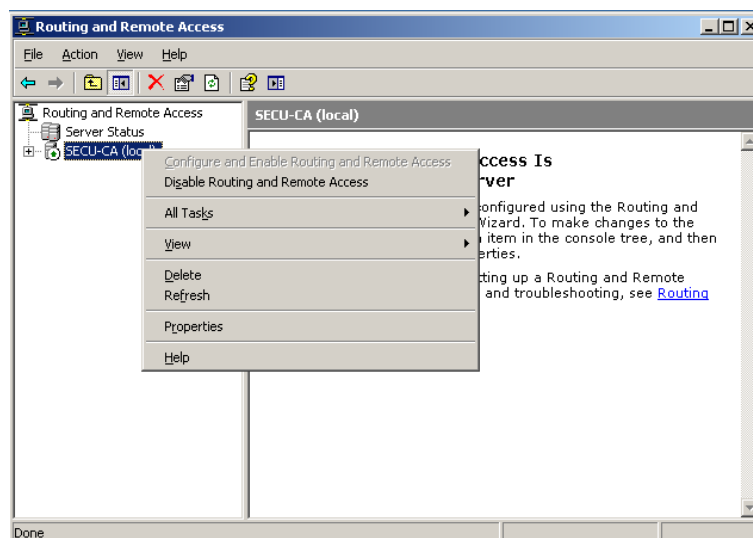
If the connection is broadband routing, it is not necessary to modify the configurations in this page.

Chapter 3: VPN Server with UniOTP

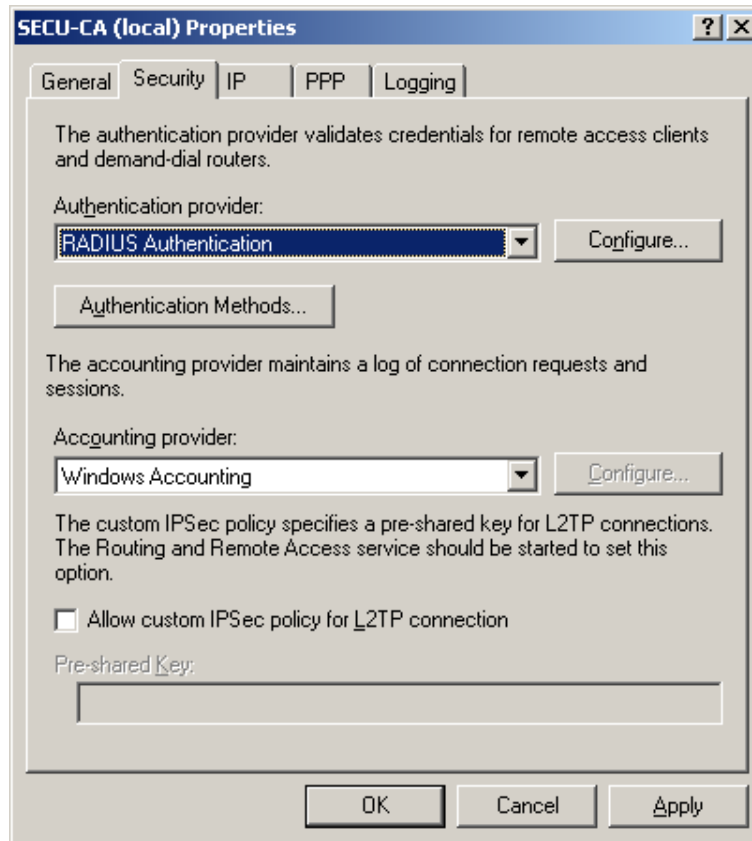
After building a VPN Server successfully, open the Start→program→administrative Tools and open the Routing and Remote Access control panel.



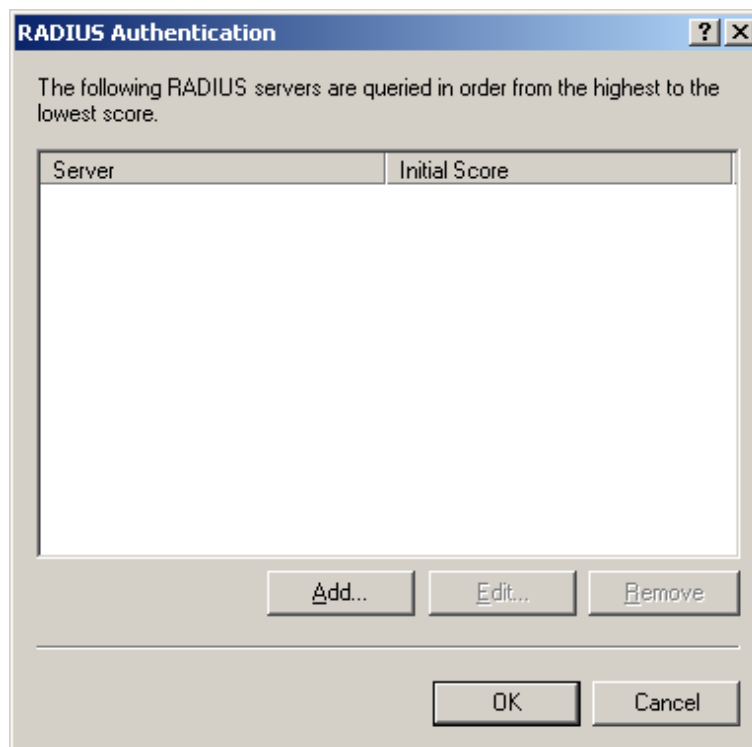
Right-click on SECU-CA (local) and select property



Select security tab, and in the authentication provider (H) list, select “Radius authentication”. The “Configure” button will now become available as the following picture shows.

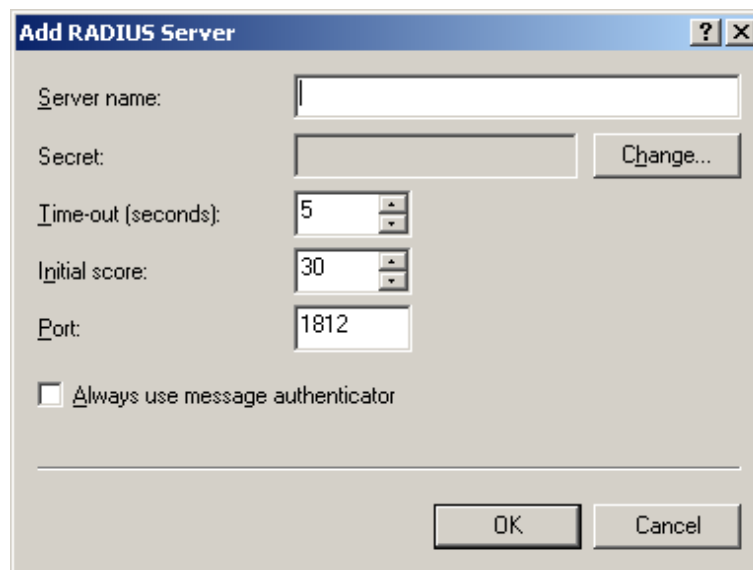


Please click on the “Configure” button to configure the Radius authentication server. The configuration panel appears.



Click on “Add” button to add a Radius authentication server.

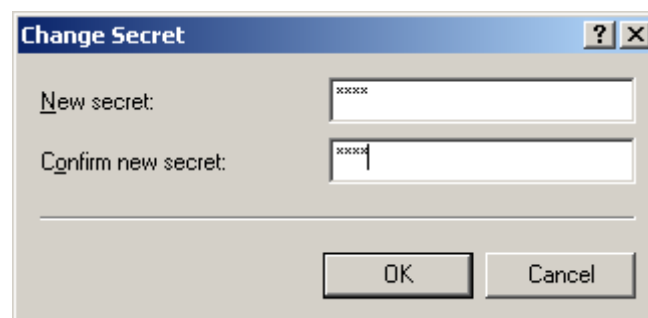
In the following configuration panel, fill the UniOTP authentication server address in Server name.



The "Add RADIUS Server" dialog box contains the following fields and controls:

- Server name:** A text input field.
- Secret:** A text input field with a "Change..." button to its right.
- Time-out (seconds):** A spin box with the value 5.
- Initial score:** A spin box with the value 30.
- Port:** A text input field with the value 1812.
- Always use message authenticator:** An unchecked checkbox.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

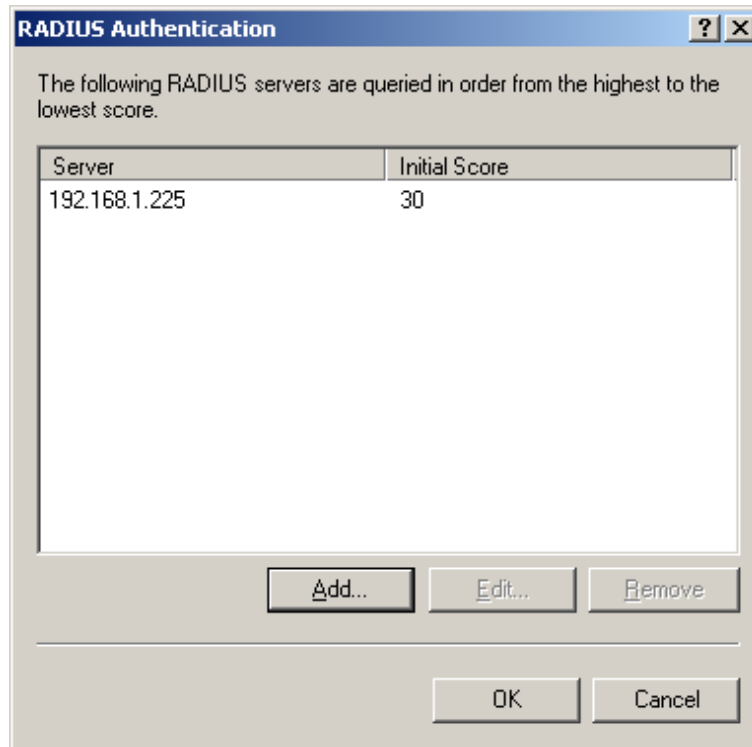
Click on "Change" to change the Radius communication shared key. As with the following picture, please configure the communication shared key



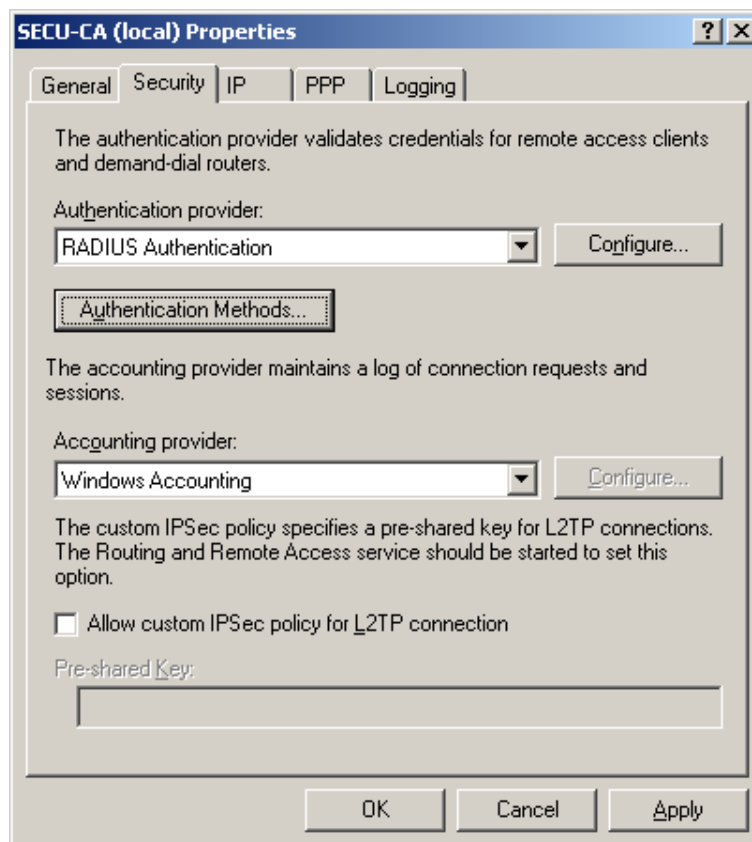
The "Change Secret" dialog box contains the following fields and controls:

- New secret:** A text input field with masked characters (xxxx).
- Confirm new secret:** A text input field with masked characters (xxxx).
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

Click on "OK" and the following content should appear indicating a Radius authentication server has been added. Click on "OK" to exit authentication server configuration.



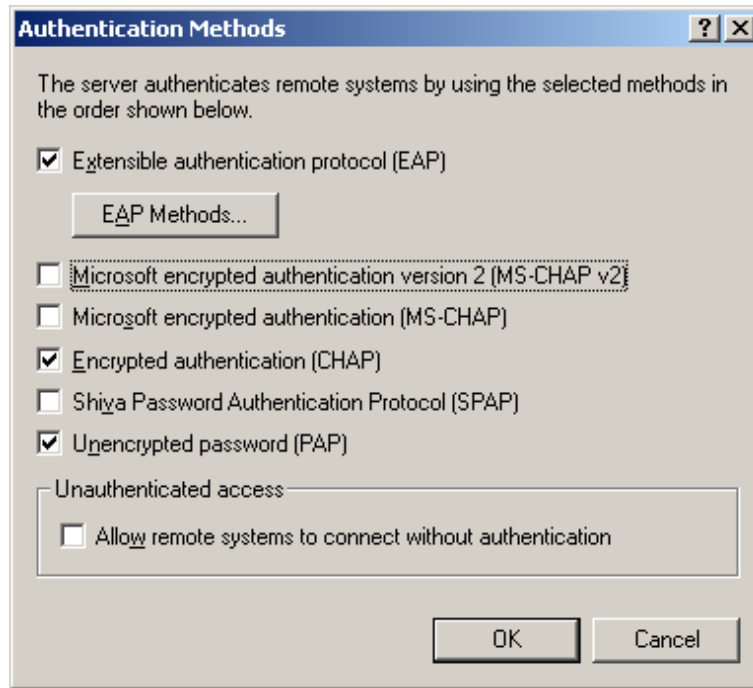
Click on “Authentication Methods” button, as in the following picture:



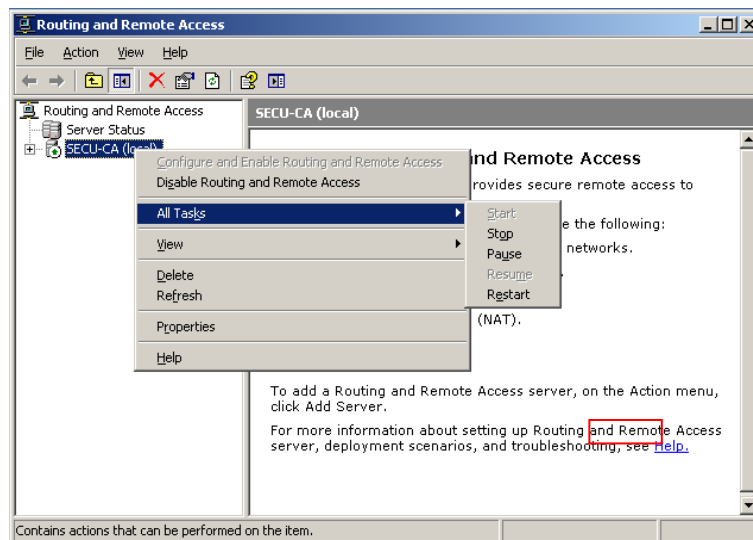
*Please note:
“MS CHAP
v2”, “MS-
CHAP” and
“SPAP”
authentication
methods are
not
supported.*

In the “Authentication Methods” control panel select “Extensible authentication protocol (EAP)”, “Encrypted authentication (CHAP)” and “Unencrypted password (PAP)”.

After configuration, click on OK → Apply and exit the control panel.

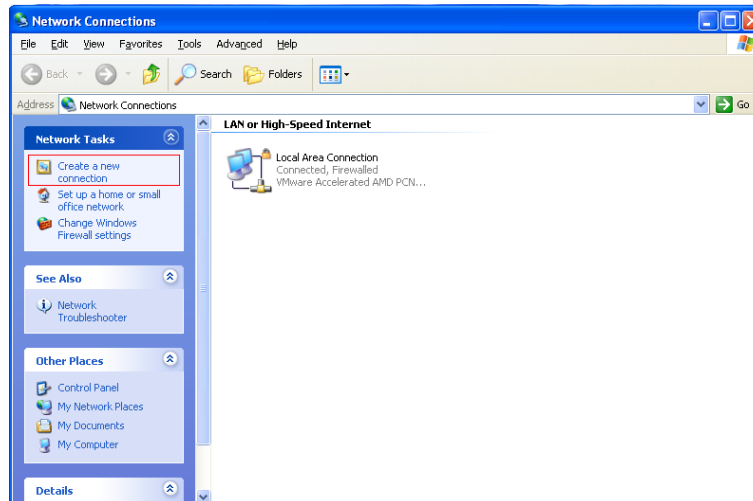


To enable new configurations, restart VPN server.

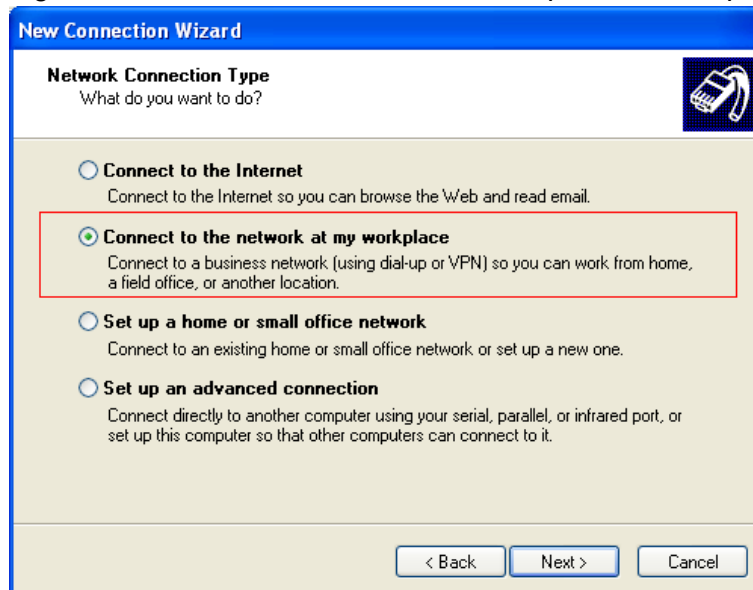


Chapter 4: Add VPN client

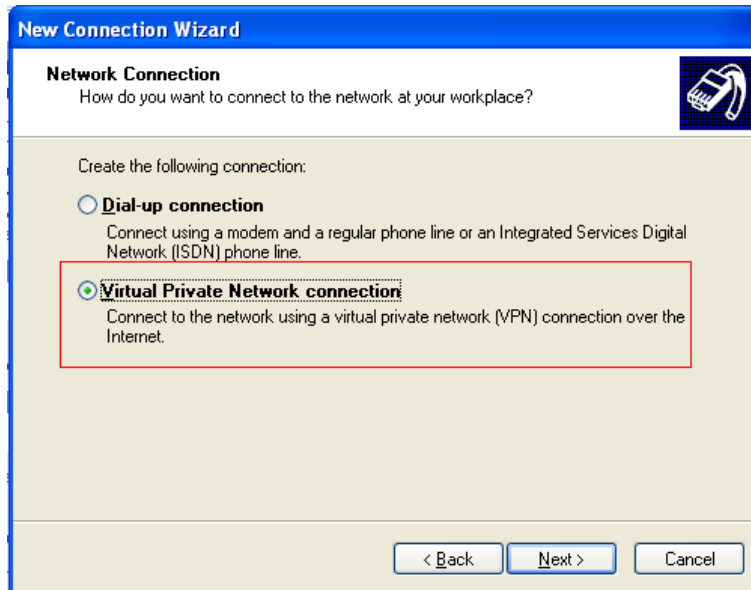
Right click on the Network icon to open network connection control panel.



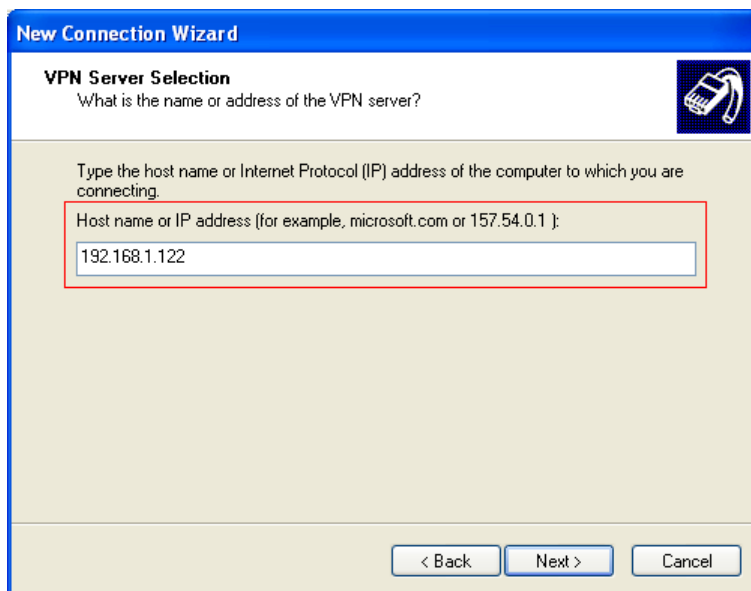
Clicking on “Create a new connection”, a set up window will pop up.



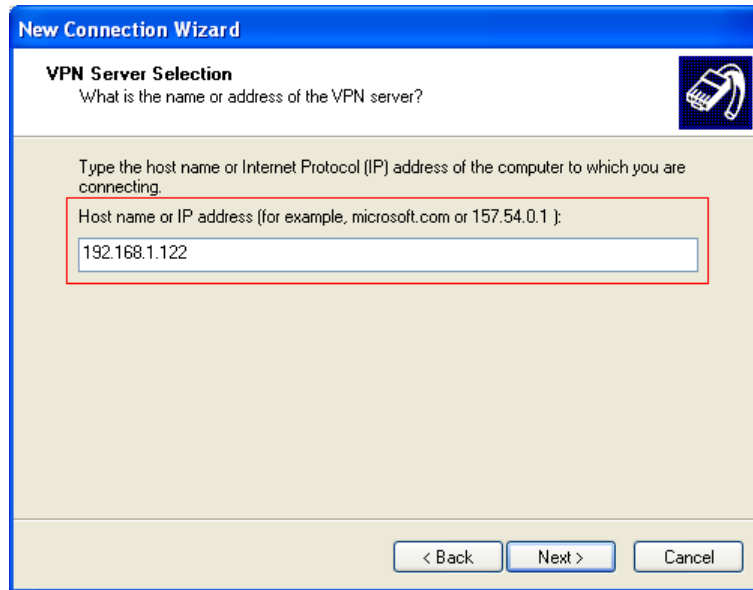
Select “Connect to the network at my workplace”, and then click “Next”



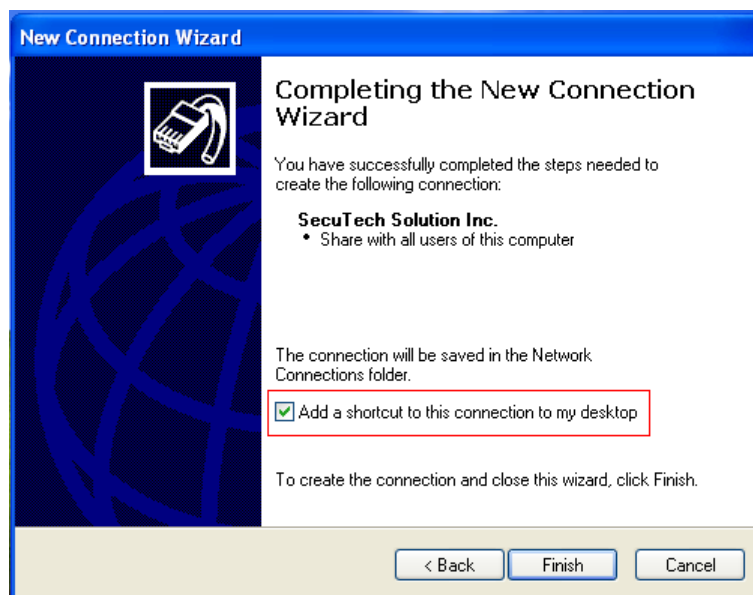
Select “Virtual Private Network connection”, and then click on “Next”



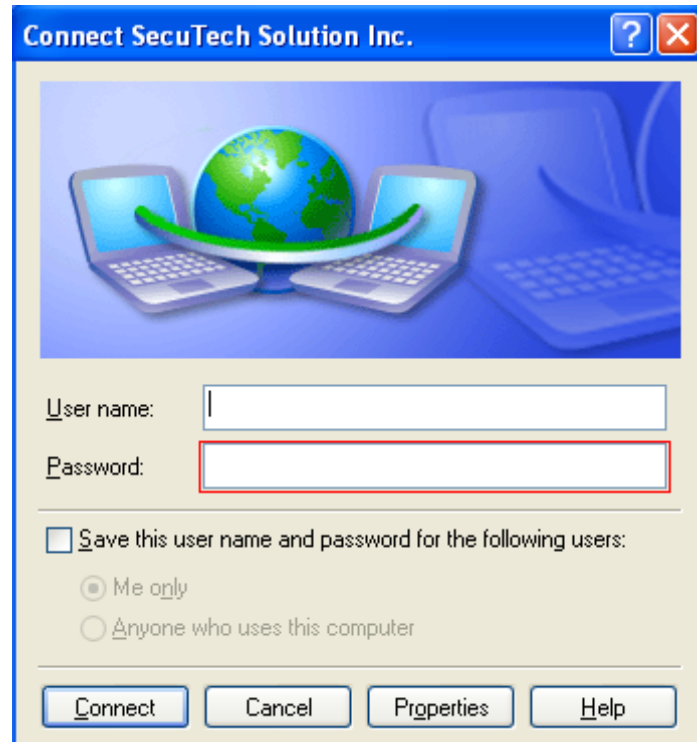
Enter the VPN name or IP address, and click on “Next”.



You can choose “Add a shortcut to this connection to my desktop” in the following window and click “Finish”.



After configuration, a window will appear.



If you have added a VPN access user, and bound this user to a dynamic token, you can use that dynamic password and PIN (if OTP+PIN authentication method has been selected) to connect to the VPN. When following this manual, a Guest account has been added to VPN Server and to the UniOTP dynamic password authentication system, therefore Guest and OTP + PIN (for Guest account the authentication method is OTP + PIN) need to be filled into this window. Please Click "Connect"



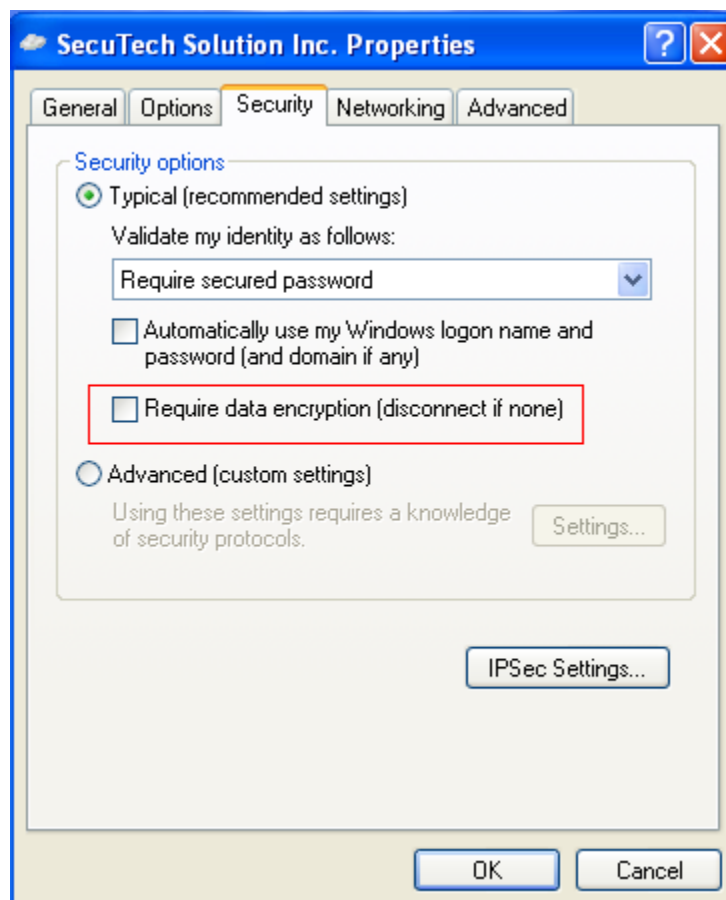
The following error may happen:



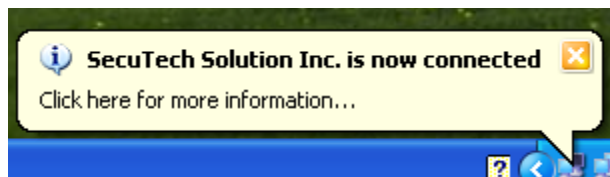
To solve this error, please click “Properties”



Unselect “Require data encryption”→click on “OK”, and click “Connect” to start connection again.



After connecting to VPN server successfully, on the lower right corner of the screen, the following information will appear indicating that the configuration of VPN with UniOTP authentication has been completed successfully.



Chapter 5: Appendix:

5.1 Common errors in VPN clients connect to server:

Error Code	Reason
800	Unable to establish the VPN connection. The VPN server may be unreachable, or security parameters may not be configured properly for this connection
619	In most cases, it is caused by that the NAT-T function used for client to connect to internet is turned off or bad VPN support that does not support NAT-T in GRE and PPTP protocol. To solve this problem, you can turn on the gateway's NAT-T. If this error happens frequently, please change the gateway equipment.
721	<p>In most cases, this problem is caused by client system. If users are using Windows XP SP2, this problem may happens, and you can solve it through modifying registry:</p> <p>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Class\{4D36E972-E325-11CE-BFC1-08002bE10318}\<000x>. <000x> is the network adapter of the Satellite WAN port (PPTP) driver. In this key, create a new DWORD value, name ValidataAddress and value 0. If the configuration of the PPP protocol on the server is not correct, it will cause this problem as well.</p>
718	Wrong user name or password when dial-up, or authentication service errors occur on authentication server.
734	Mostly it is caused by VPN configuration problem, such like PPP configuration, unsupported or bad supported MPPE.

Follow us!



[Twitter](#)



[Facebook](#)



[Youtube](#)



[Linked in](#)



About SecuTech

SecuTech Solution Inc. is a company specializing in data protection and strong authentication, providing total customer satisfaction in security systems & services for banks, financial institutions & other industries. Having extensive and in-depth experience within the information security market, SecuTech has drawn upon this experience to utilize today's cutting-edge technologies, enables enterprises, financial institutions, and government to safely adopt the economic benefits of mobile and cloud computing that are effective against increasingly sophisticated cyber attacks.

SecuTech www.eSecuTech.com SecuTech Solution Inc.

North America

1250 Boulevard René-
Lévesque Ouest, #2200,
Montreal, QC, H3B 4W8,
Canada
T: +1 -888-259-5825
F: +1 -888-259-5825 ext.0
E: INFO@eSecuTech.com

China

Level 12, #67 Bei Si Huan
Xi Lu,
Beijing, China, 100080
T: +8610-8288 8834
F: + 8610-8288 8834
E: CN@eSecuTech.com

APAC

Suite 5.14, 32 Delhi Rd,
North Ryde,
NSW, 2113, Australia
T: 00612-9888 6185
F: 00612-9888 6185
E: AUS@eSecuTech.com

EMEA

4 Cours Bayard 69002
Lyon, France
T: +33-042-600-2810
F: +33-042-600-2810
M: +33-060-939 6463
E: Europe@eSecuTech.com

©Copyright 2012 SecuTech Solution Inc. All rights reserved. Reproduction in whole or in part without written permission from SecuTech is prohibited. SecuTech UniOTP and the SecuTech logo are trademarks of SecuTech Inc. Windows and all other trademarks are properties of their respective owners. Features and specifications are subject to change without notice.