

UNIOTP SERVER CONTROL 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	2011.1.30
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: INSTALLATION	2
1.1 Installation	2
CHAPTER 2: UNIOTP SERVER CONTROL	3
2.1 User Interface	3
CHAPTER 3: DATABASE CONFIGURATION	4
CHAPTER 4: AUTHENTICATION SERVICE CONFIGURATION	6
CHAPTER 5: LOG AND AUTHENTICATION PARAMETERS CONFIGURATION	7
CHAPTER 6: SHARED SECRET KEY FOR AUTHENTICATION SERVICE AND CLIENTS	8
CHAPTER 7: EMAIL PARAMETER CONFIGURATION	11
CHAPTER 8: EXIT THE TOOL	12

About this guide

UniOTP Server Control is a desktop tool used to configure and manage the UniOTP authentication service. By using this tool, you can check and control the status of UniOTP authentication service, as well as check and reconfigure the configuration information of the UniOTP authentication service.

This document is intended for the network administrator and users who manage and configure the authentication service.

Chapter 1: Installation

1.1 Installation

To install the UniOTP Server Control, please install UniOTP Authentication Server Installation\Windows\UniOTP Server.exe.

Please insure that a database is installed and that the proper ODBC drivers have been configured for the UniOTP database. Initiate database list for UniOTP dynamic password authentication system by using the corresponding SQL initiation file in the "initsqlscript" folder.

Once installation is complete, please navigate to the otp_conf.conf file (by default, located in "C:\Program Files \UniOTP\1.0\config").

Several parameters need to be configured:

[DataBase]

Data source nameotp_dsn=

Dabase user anme otp_uid=

Database user password otp_pwd=

Database type otp_dbtype=

[share]

Radius shared key format is IP=share, where IP is the Radius client IP address, the computer IP address which has UniOTP Agent installed is the shared key to the corresponding computer with the specified IP address. Assigning shared key to 0.0.0.0, you can set shared key for all clients whose shared keys have not been set. For example:

0.0.0.0=hello

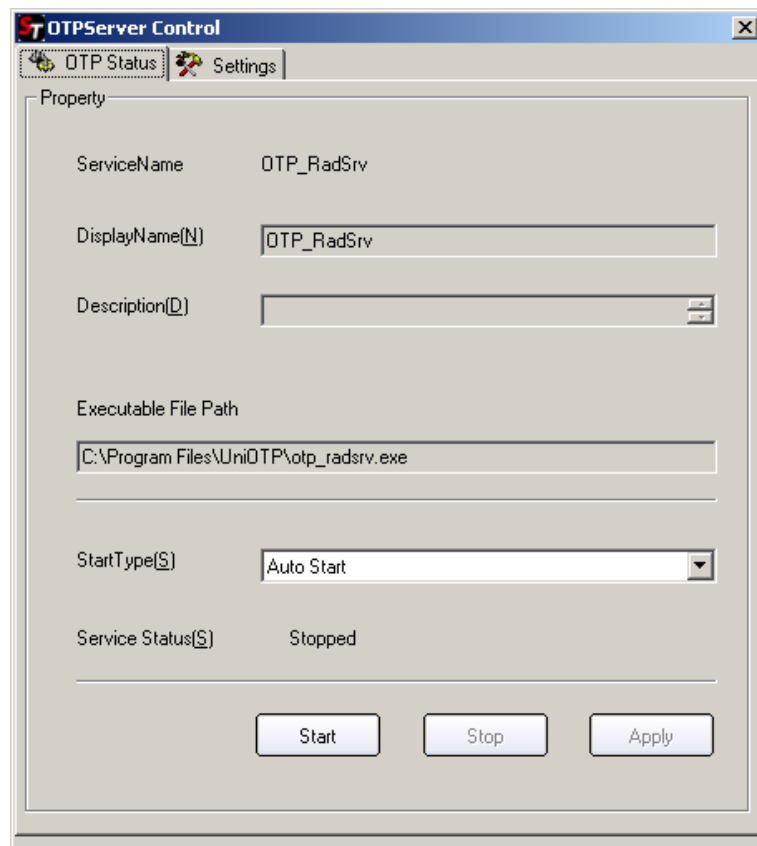
192.168.1.100=hi

The shared key to Client with IP address192.168.1.100 is hi, and for other clients, hello will be used as the shared key.

Chapter 2: UniOTP Server Control

2.1 User Interface

Once the program has started, the following will appear:



After the program has started, the OTP Status tab will appear:

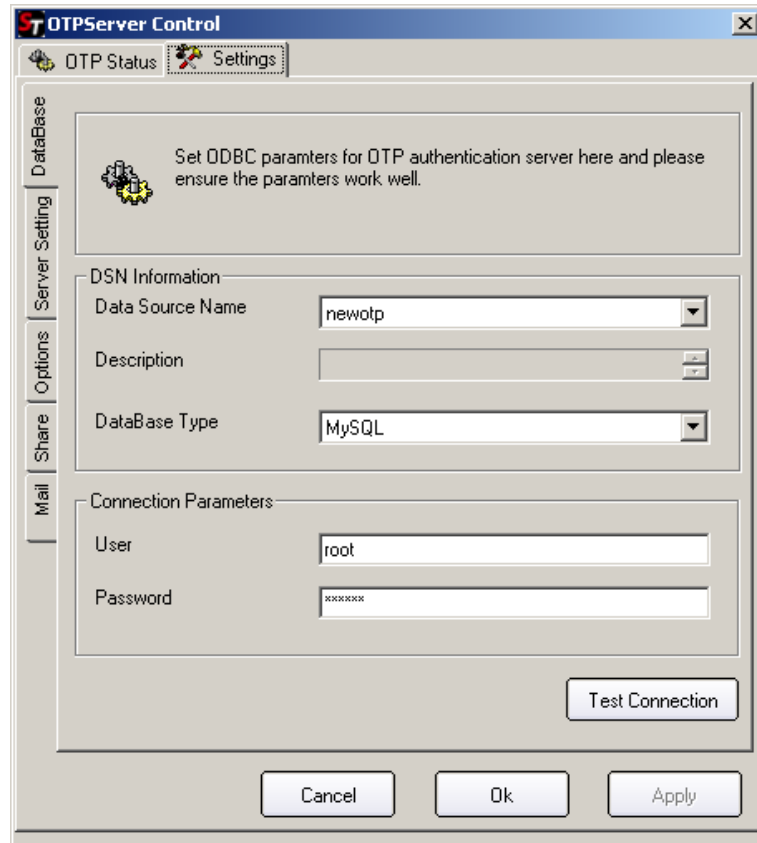
- **ServiceName:** Name of service
- **DisplayName:** The display name of service
- **Description:** The description information of the service
- **Executable File Path:** The absolute path of the executable program corresponding to the service
- **StartType:** The start type of the service. It can be set to automatic, manual or disable
- **Service Status:** The service's current status

After the service configuration is changed, the Apply button will become available, and click on Apply to apply the new configuration.

Click on Start or Stop to start and stop the service.

Chapter 3: Database configuration

In the settings tab, there are more service configuration interfaces:



DSN Information is used to configure the data source

- **Data Source Name:** Select the suitable database source
- **Description:** Description of the database source
- **DataBase Type:** The type of database

Connection Parameters is used to configure the database link parameters

- **User:** The username used to connect the database
- **Password:** The login database password corresponding to the user

After configuring all parameters, please click on the “Test Connection” button to test the connection.

If all the information is valid, the connection has succeeded, as shown in the following picture.

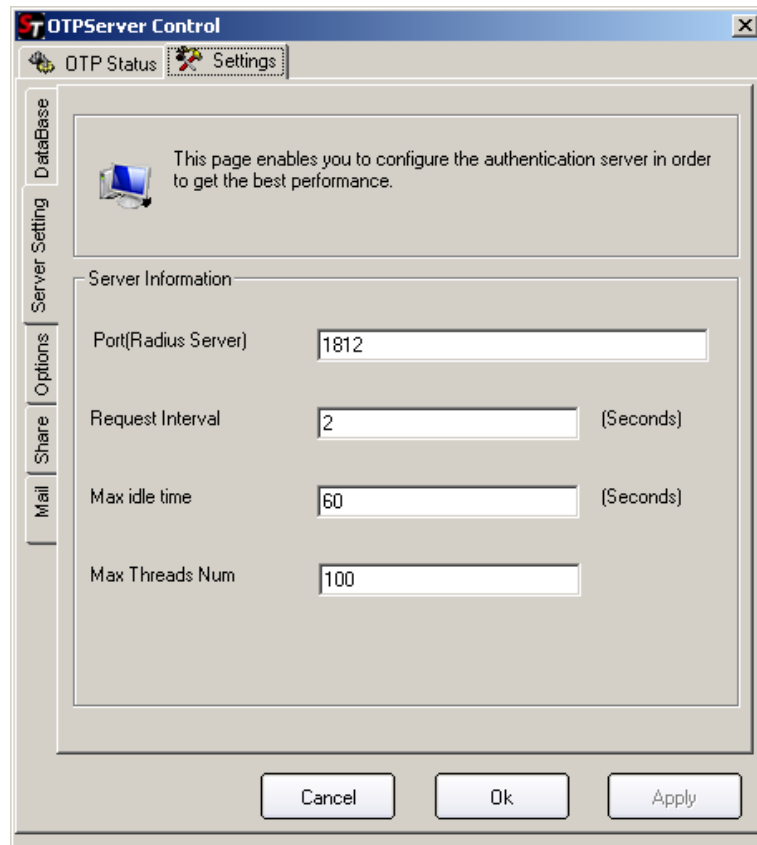


If the information is wrong, the connection will failure, as shown in the following picture.



Chapter 4: Authentication service configuration

Click on “Server Setting” tab to switch to service configuration interface, as the following picture.



The Server Information column contains configuration information about service network and performance.

The default port is 1812

Port (Radius Server): the port number of the authentication service, following the Radius authentication protocol.

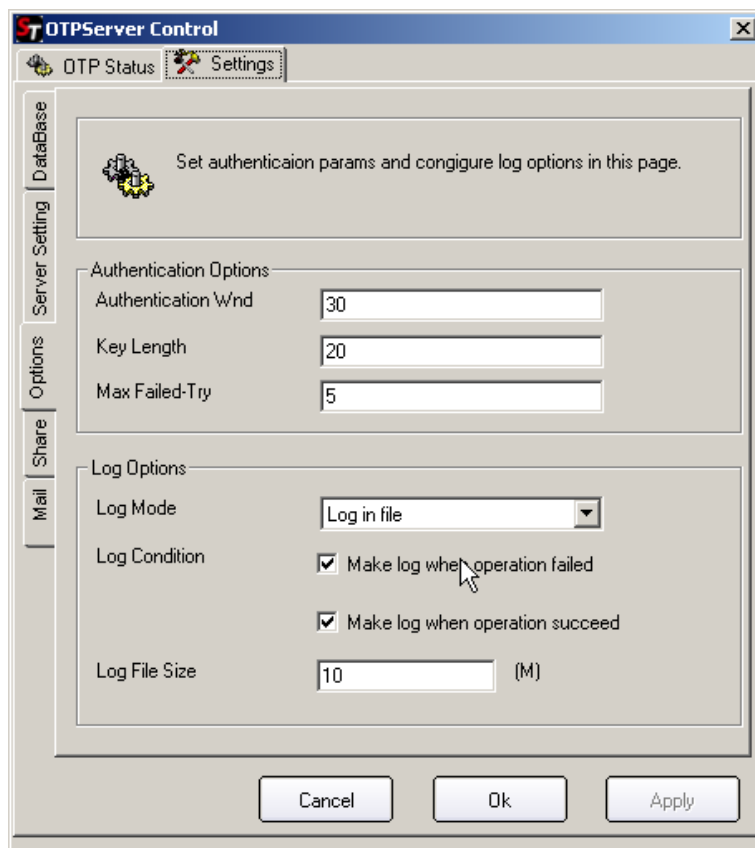
Request Interval: Period of time between requests

Max idle time: The maximum idle time of the certified thread

Max Threads Num: The maximum number of worker threads.

Chapter 5: Log and authentication parameters configuration

Select “Options” tab to enter log and authentication parameters configuration, as the following picture.



In Authentication Option column configure

- **Authentication Wnd:** Authentication window, the default value is 30 (for safety reasons the window should not be set too big)
- **Key Length:** The length of user secret key (please change this value carefully)
- **Max Failed-Try:** The maximum number of failure attempts

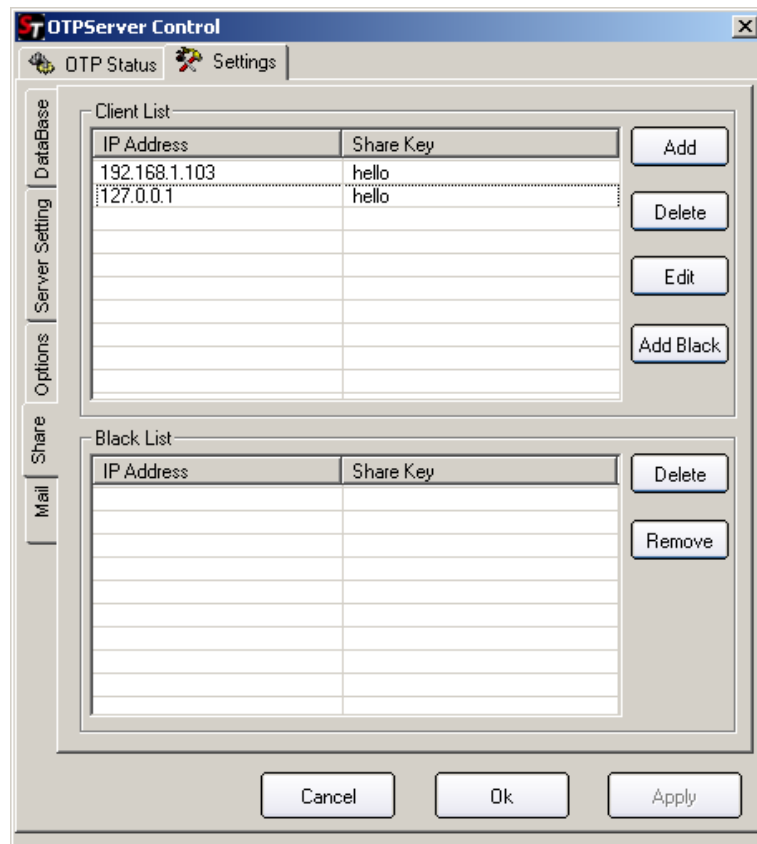
In the Log Options column, configure log mode

- **Log Mode:** Log mode (store the log in log file or database)
- **Log Condition:** The condition of log generation
- **Log File Size:** Maximum log file size when you choose to store log in log file

Chapter 6: Shared secret key for authentication service and clients

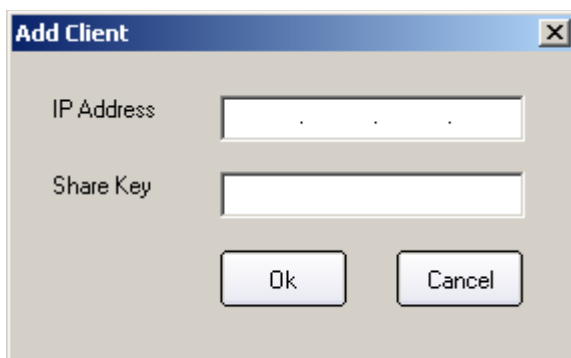
Click on Share tab to enter the shared secret key configuration interface.

In this panel, configure the shared secret key of the authentication client (application server), and enable/disable status.



In the Client List, the IP address shows the current authorized authentication clients and shared Key displays the shared secret key for the service and the current authentication client.

Click on the “Add” button to add a new authentication client. Enter a new client IP address and shared key. After adding a new authentication client, click on Apply to save and apply the new configuration.



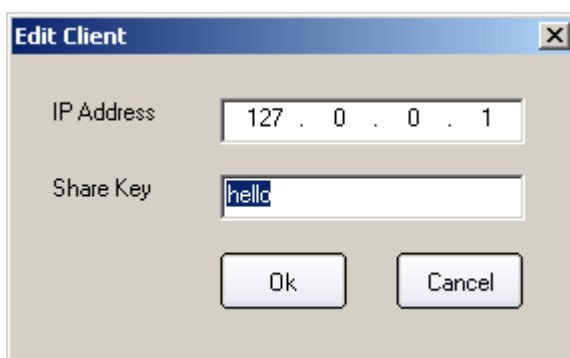
Click on the “Delete” button to delete an authentication client. After clicking on delete, the selected client will be deleted. During the delete operation, a confirmation dialogue will pop up.



If no client is selected, the following reminding message will appear.



Click on the “Edit” button to modify the configuration of the selected client. The client IP address will not be modified, and only the shared key can be changed. For example, if the client (IP address 127.0.0.1) is selected, after clicking on edit, a dialogue window will pop up. Enter the new shared key in the dialogue, and then the Apply button will become available. Click Apply to enable all the new configurations.



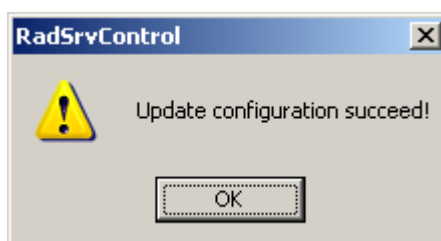
Click on Add Black button to add an authentication client to black list. The client in the black list will not request authentication, but the authentication system will save the relative shared key information, so the authentication function can be recovered by removing the client from the blacklist.

In the Black List, the IP addresses displays all the authentication clients IP address added into the blacklist, and shared key displays the shared key for the client and the authentication service.

Click on the Delete button to delete an authentication client from the blacklist. After operator confirms the delete operation, the client will be permanently deleted from the system.

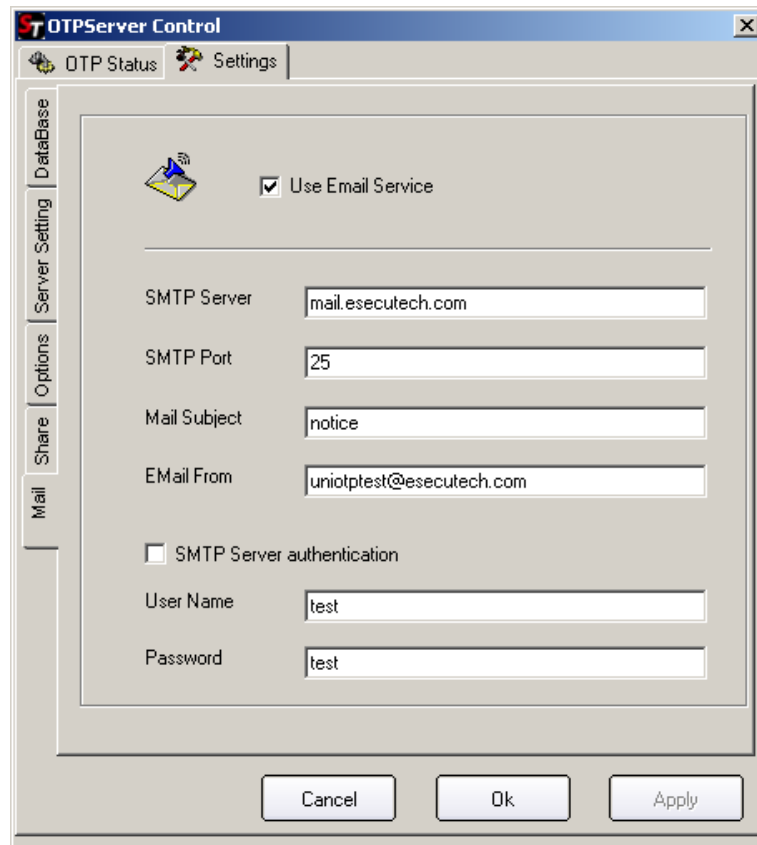
Click on the “Remove” button to remove the client from the blacklist, to recover the authentication. After executing the remove operation, click on “Apply” to apply changes.

After clicking on Apply, the following message will appear:



Chapter 7: Email parameter configuration

Click on Mail tab to enter Email configuration interface. This panel contains configurations about the Email server.



Use Email Service select box to decide whether use email reminding function.

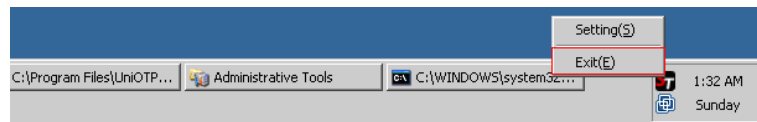
After using the email reminding function, the SMTP server must be configured.

- **SMTP Server:** SMTP server name or IP address
- **SMTP Port:** SMTP server Port (default port is 25)
- **Mail Subject:** The mail subject sent by the system
- **Email From:** The email address displayed to email recipients
- **SMTP Server authentication:** Authentication of email server
 - User Name:** Username used for SMTP authentication.
 - Password:** Password corresponding to the User name.

After finishing configuration, click on the “Apply” button to apply configurations.

Chapter 8: Exit the tool

The tool will not exit by clicking on the close button in the interface. The tools just minimize to the tray. Right click on the icon in the tray, and click on Exit to close the program, as shown in the following picture.



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.