

UniOTP Server Control Tool

Contents

About this tool.....	2
Intorduction.....	2
Audience	2
How to use this tool	2
Launch the tool	2
Function introduction.....	2
Service status control	2
Database configuration	3
Authentication service configuration	5
Log and authentication parameters configuration.....	5
The configuration of the shared secret key for the authentication service and clients	6
Email parameters configuration	9
Exit the tool.....	10

About this tool

Intorduction

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

Audience

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

How to use this tool

Launch the tool

1. Double click on UniOTPSCRControl desktop shortcut to launch service control program.
2. Launch the service control program through Start->Programs->UniOTPSCRControl

Function introduction

Service status control

After the program is started, the interface of the service status will appear.

ServiceName: name of service

DisplayName: the display name of service

Description: the description information of the service

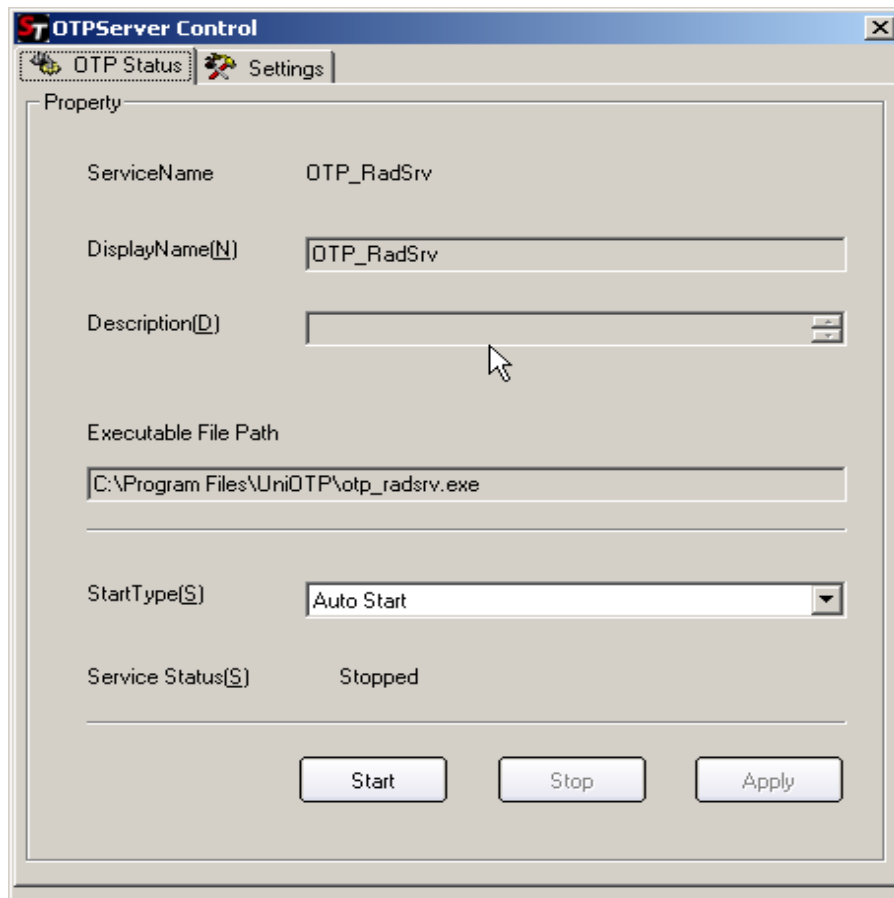
Executable File Path: the absolute path of the executable program corresponding to the service

StartType: the start type of the service. It can be set to automatic, manual and disable

Service Status: the service 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.



Database configuration

Click on Settings tab to get into more service configuration interfaces, such like the database configuration interface, as the following picture.

DSN Information is used to configure the data source

Database Source Name: select the suitable database source

Description: description of the database source

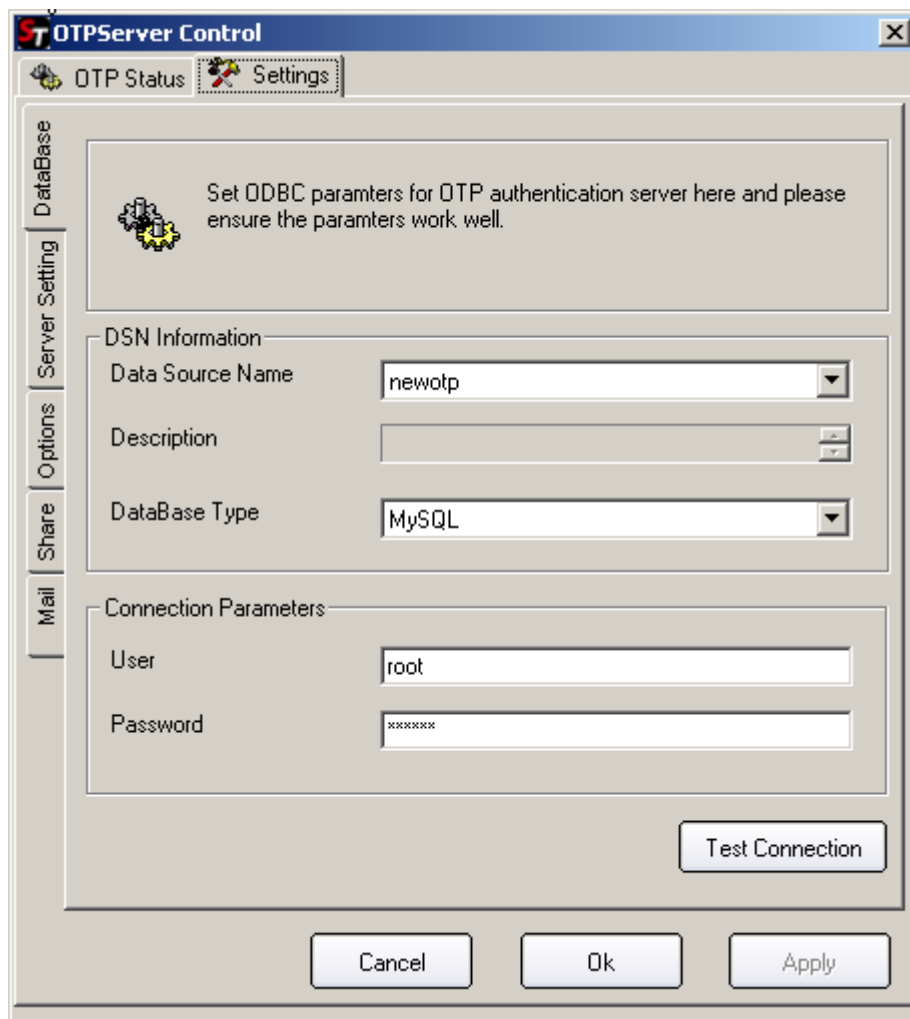
DataBase Type: the type of database

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

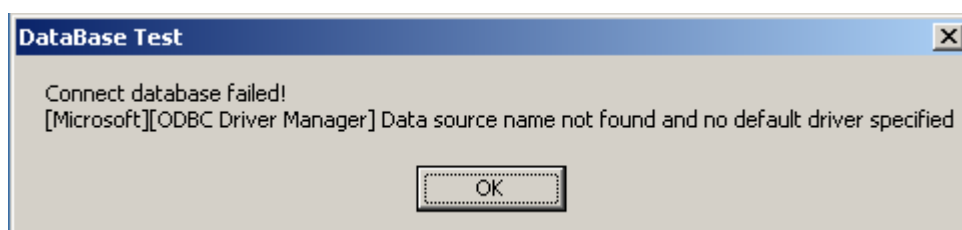
After configuring all parameters, click on "Test Connection" button to test the connection.



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



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



Authentication service configuration

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

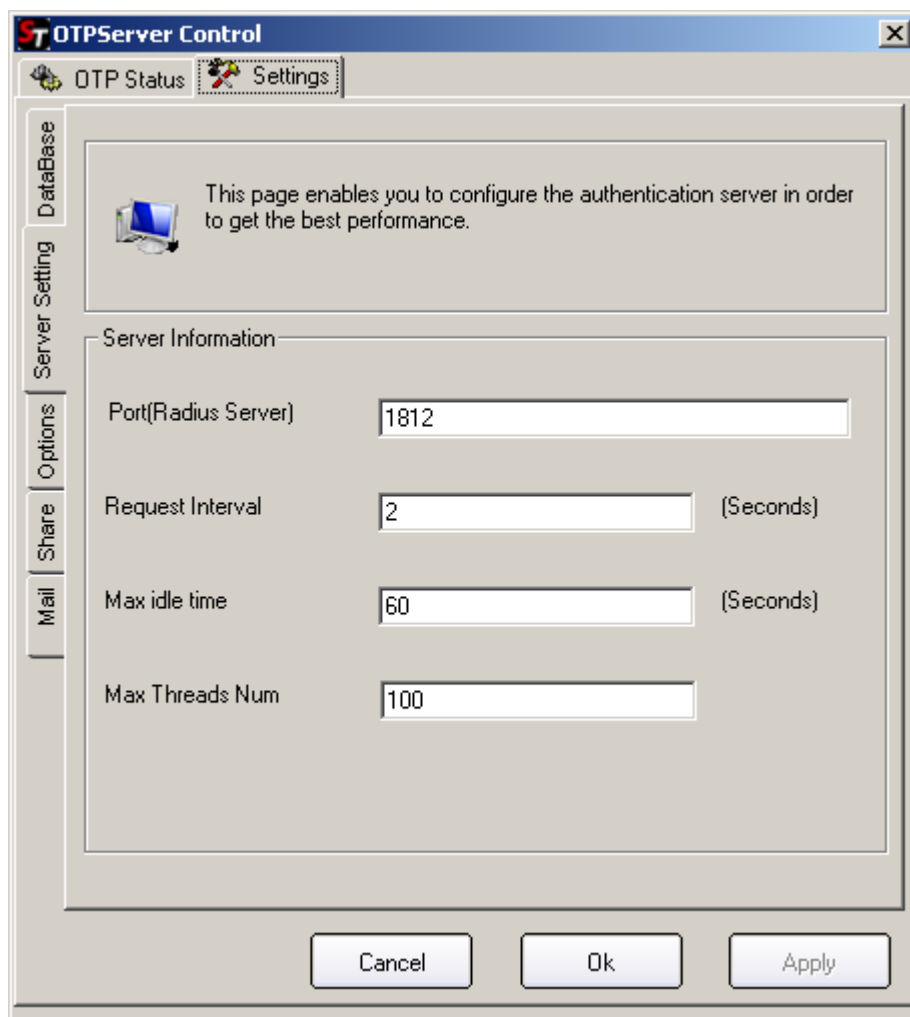
The Server Information column contains configuration information about service network and performance.

Port (Radius Server): the port number of the authentication service, following the Radius authentication protocol. The default port is 1812.

Request Interval: the 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.



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 to big)

Key Length: the length of user secret key (please change this value carefully)

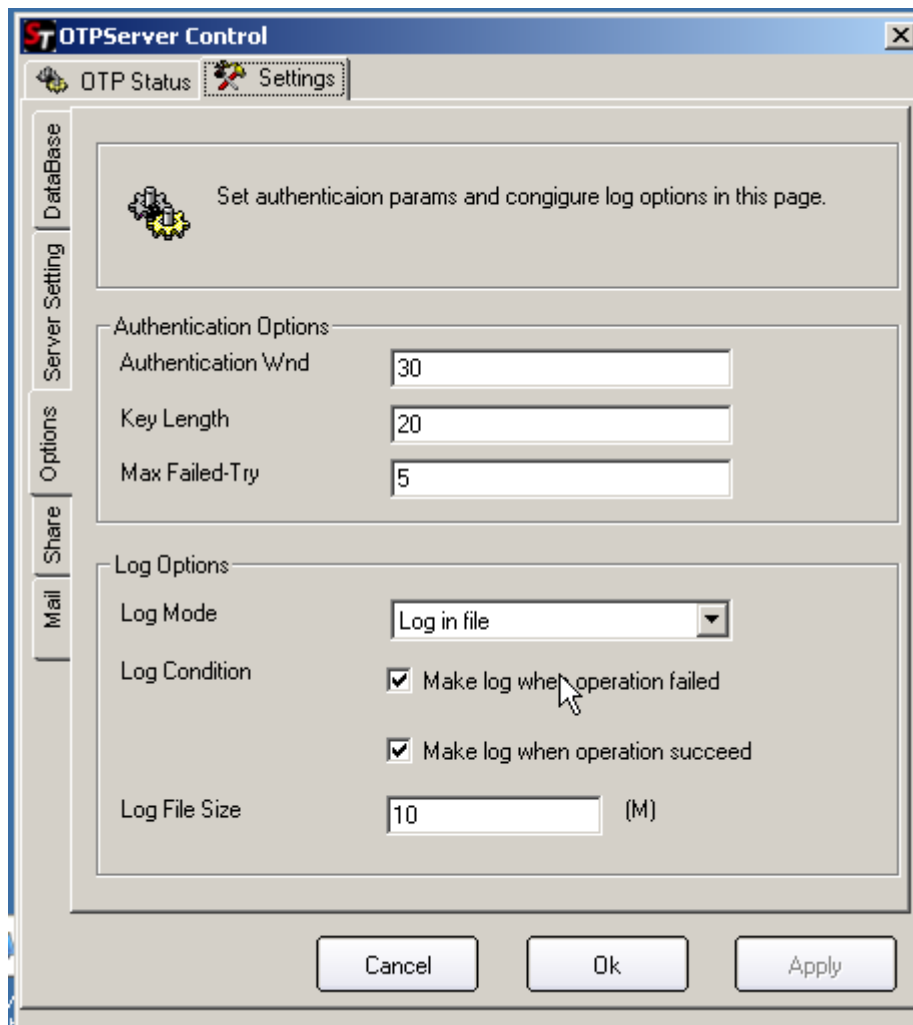
Max Failed-Try: the maximum number of failure attempts

In the Log Options column, configure lag mode

Log Mode: log mode (store the log in log file or database)

Log Condition: the condition of log generation

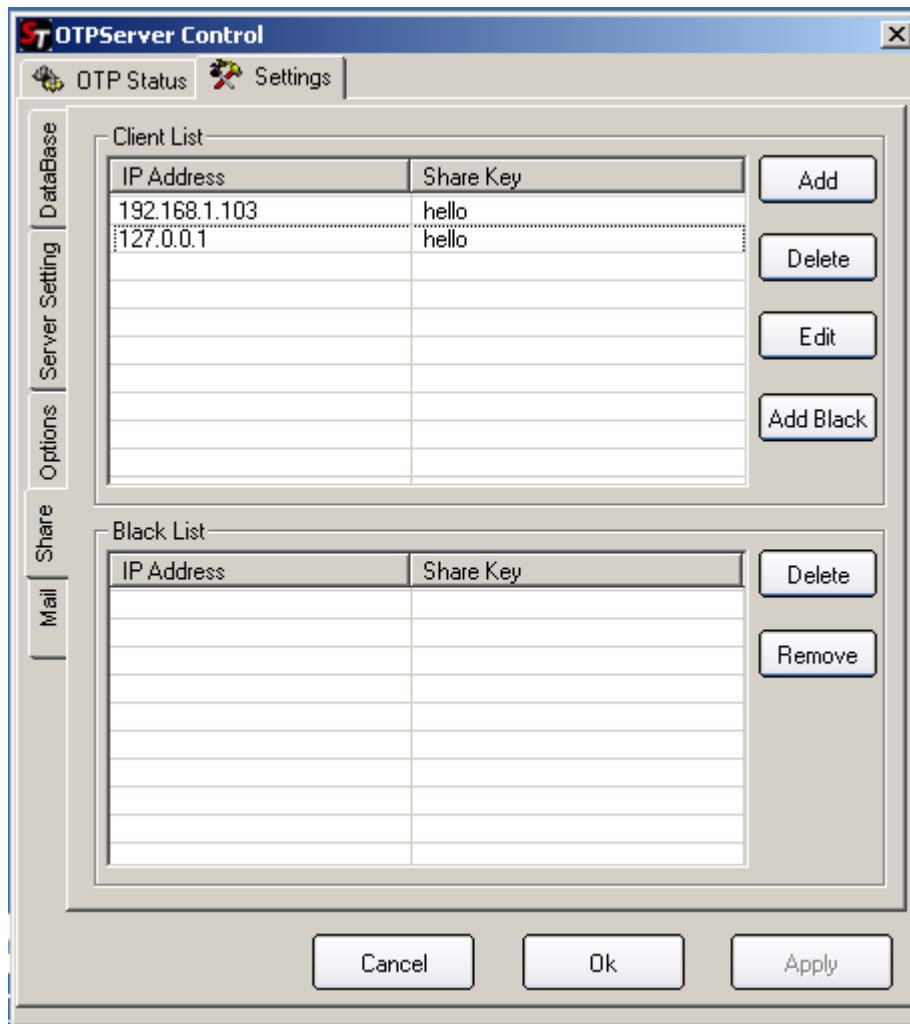
Log File Size: the maximum log file size when you choose to store log in log file



The configuration of the shared secret key for the authentication service and clients

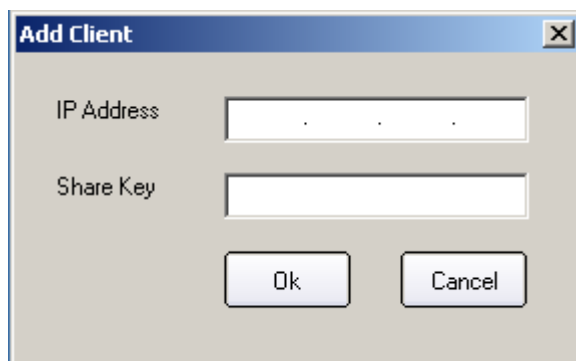
Click on Share tab to enter shared secret key configuration interface.

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

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

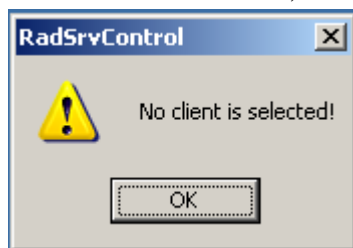


Click on Delete button to delete an authentication client. After click on delete, the selected client will be deleted. During the delete operation, a confirmation dialogue will pop up (after confirm the delete operation, the client configuration file will be

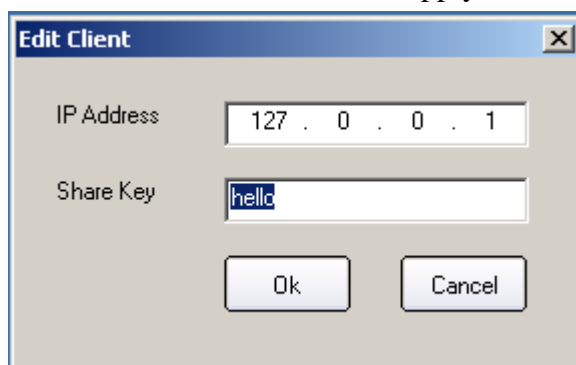
deleted)



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



Click on Edit button to modify the configuration of the selected client. The client IP 按 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 click on edit button, a dialogue window will pop up. Enter the new shared key in the dialogue, and then the Apply button will become available. Click Apply button to enable all the new configurations.



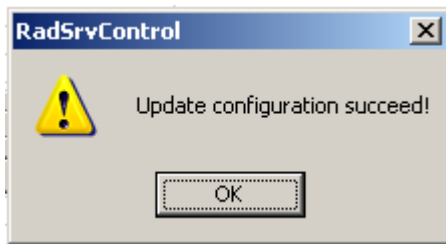
Click on Add Black button to add an authentication client to black list. The client in the black list will not request authentication, but the authentication system will save the relative shared key information, so the authentication function can be recovered by removing the client from the blacklist.

The Black List, the IP address 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.

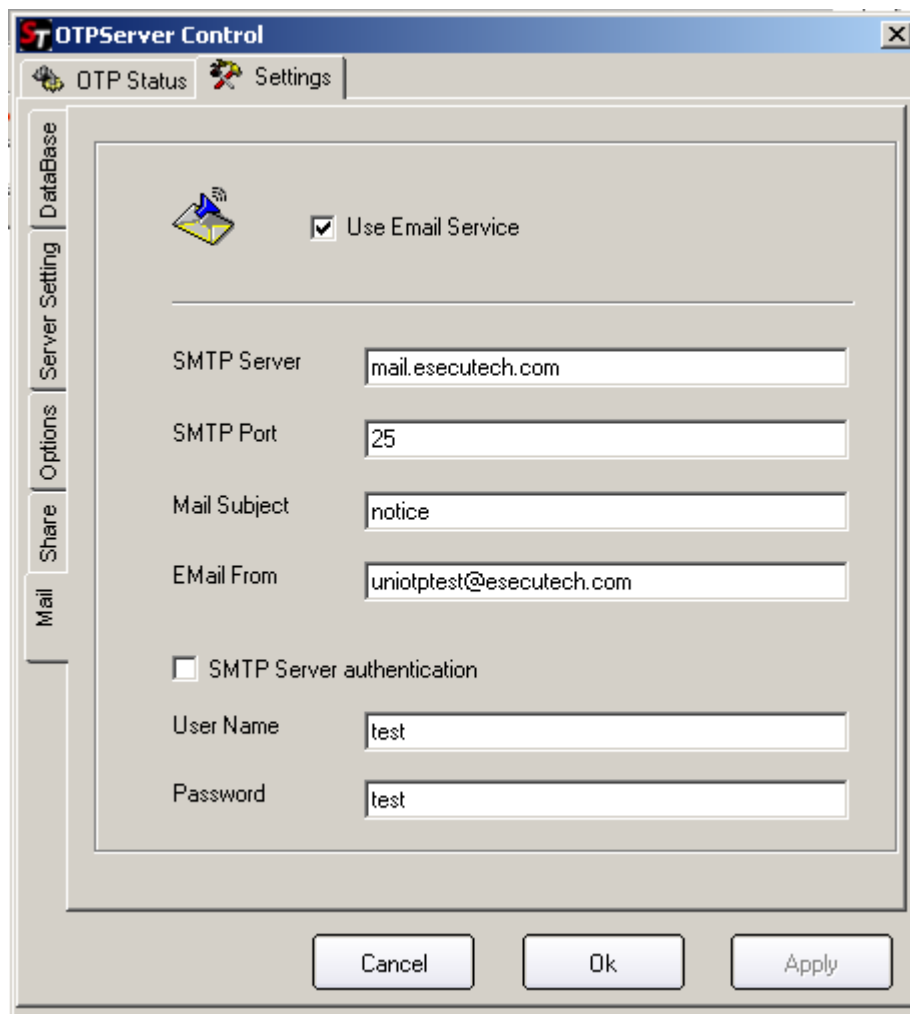
Click on Remove button to remove the client from the blacklist, to recover the authentication. After execute remove operation, click on Apply to apply changes.

After clicking on Apply, the following dialogue will appear.



Email parameters configuration

Click on Mail tab to enter Email configuration interface. This panel contains configurations about 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: the SMTP server name or IP address

SMTP Port: SMTP server Port (the default port is 25)

Mail Subject: the mail subject sent by the system

Email From: the email address displays in email recipients

SMTP Server authentication: select if the email server needs authentication

User Name: the username used for SMTP authentication.

Password: the password corresponding to the User name.

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

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.

