Futronic Technology Company Ltd.

Finger Authentication Server

User's Guide

Version 5.7

Copyright © 2003-2010 Futronic Technology Company Ltd.

Copyright © 2003-2010 Futronic Technology Company Ltd.
All rights reserved

The software contains proprietary information of Futronic Technology Company Ltd.; it is provided under a license agreement containing restrictions on use and disclosure and is also protected by copyright law. Reverse engineering of the software is prohibited.

Due to continued product development this information is subject to change without notice. The information and intellectual property contained herein is confidential between Futronic Technology Company Ltd. and the client and remains the exclusive property of Futronic Technology Company Ltd. If you find any problems in the documentation, please report them to us in writing. Futronic Technology Company Ltd. does not warrant that this document is error-free.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying and recording or otherwise without the prior written permission of Futronic Technology Company Ltd.

All the product names mentioned in this Guide are trademarks or registered trademarks of their respective owners. Futronic Technology Company Ltd. acknowledges any and all rights of the trademarked companies.

Contents

Contents 3
Section 1. Introduction 4
Section 2. Installation 5
Section 3. Un-installation 12
Section 4. Getting Started 13
Section 5. FAS Backup Utility 35
Section 6. FAS SQL Server ODBC Connection Utility 40
Section 7. Upgrade 41

Section 1. Introduction

Thank you for using Futronic Finger Authentication Server software and fingerprint scanner.

We present you an innovative product based on biometric technology, which is developed on the basis of the latest developments and advanced technologies in the field.

Finger Authentication Server (FAS) is the software developed with our fingerprint recognize algorithm. It works as a server in the TCP/IP network. It can be used to control the Logical Access with our fingerprint scanner FS80, such as Samba Client to logon to Samba Server in Linux environment. It can also be used to control Physical Access with our door lock product (Fin'Lock FS20, FS21M and FS22), which includes the user access log management. The administrative tools adopt the web base interface, after installed the web logon client, the administrator can logon to FAS at anytime from anywhere through Microsoft Internet Explorer (IE).

Futronic FAS include 2 software, Server side software **Finger Authentication Server** and Client side software **FASWebAdminClient**. Server side software is installed in the server pc, and client side software can be installed in server pc or client pc, which is used to manage the FAS server through IE.

If you have any question about our product, please call 852-24087705 or email to inquiry@futronic-tech.com
.

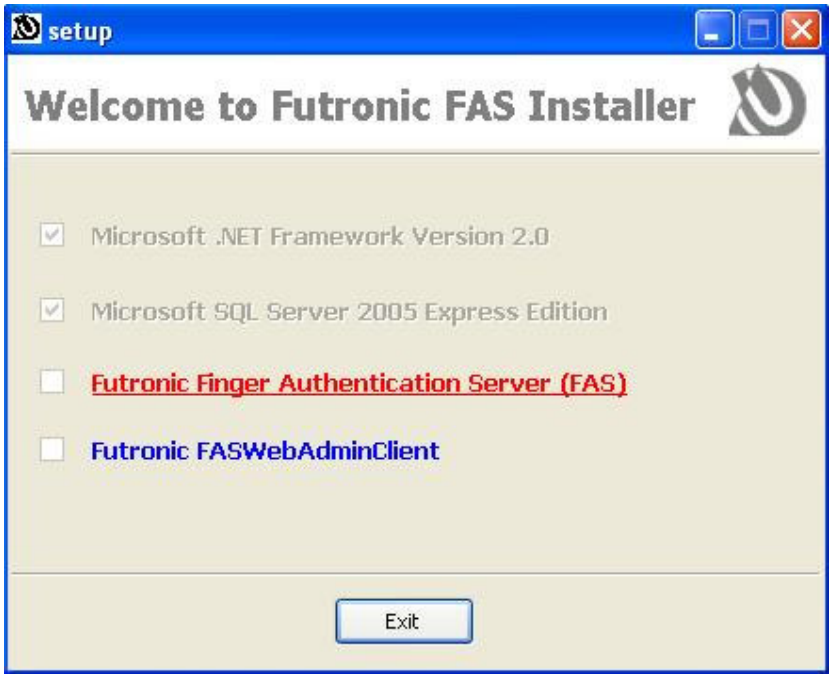
Section 2. Installation

Before installation, ensure your system meets the following requirements:

- Processor: Pentium III compatible processor 600MHz or higher required
- RAM: minimum192 MB, recommended 512 MB or more
- Screen Resolution: 16-bit color quality, 800x600 pixels or more
- Operating System: Windows 2000, Windows XP\2003\2008\Vista 32bit and 64bit, Windows 7 RC 32bit and 64bit.

Finger Authentication Server works with the database of Microsoft SQL Server, it supports **MS SQL Server 2005**.

Microsoft SQL Server Express 2005 is including in the installation CD, before installing FAS, you need to install the SQL Server. Launch the program **setup.exe** from the CDROM included in the package of the product. It will detect your OS and show the items that you need to install, please click the enabled item to install the related software.



2.1 Install Microsoft .NET Framework Version 2.0

Microsoft .NET Framework version 2.0 is required by SQL Server 2005, before installing the SQL server, you need to install .NET framework. Please follow the instruction to install it.

2.2 Install Microsoft SQL Server 2005 Express Edition

FAS version 4.0 or above use the SQL server as the background database, before installing the FAS, you need to install MS SQL server. Please follow the instruction to install it.

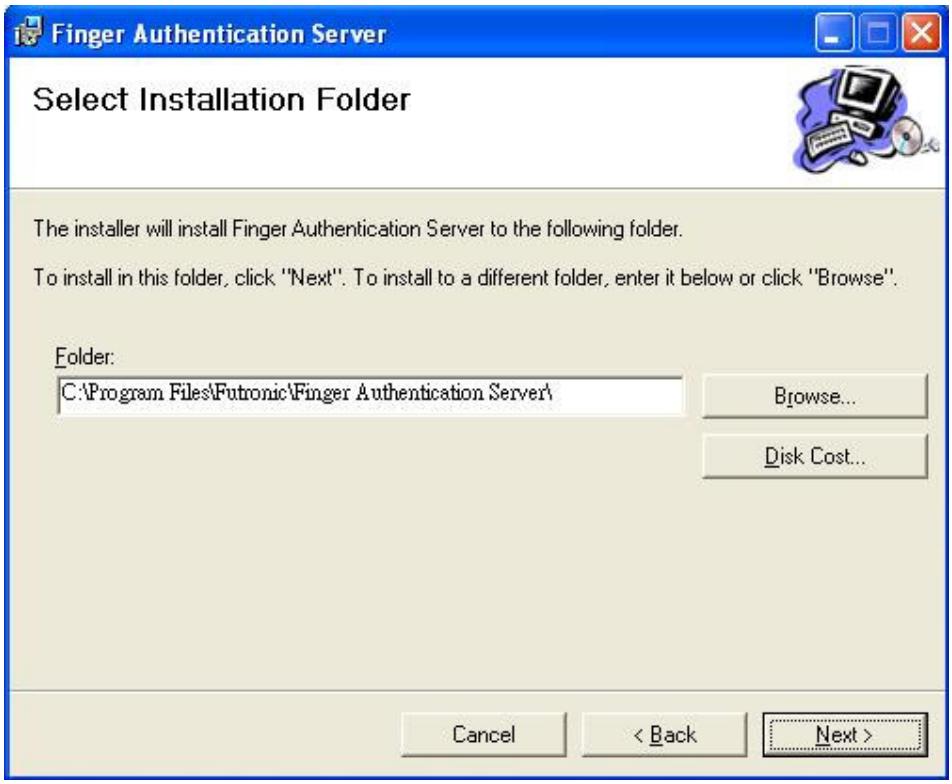
2.3 Server Side Software – Finger Authentication Server

The Server Side Software is installed in the server pc only.

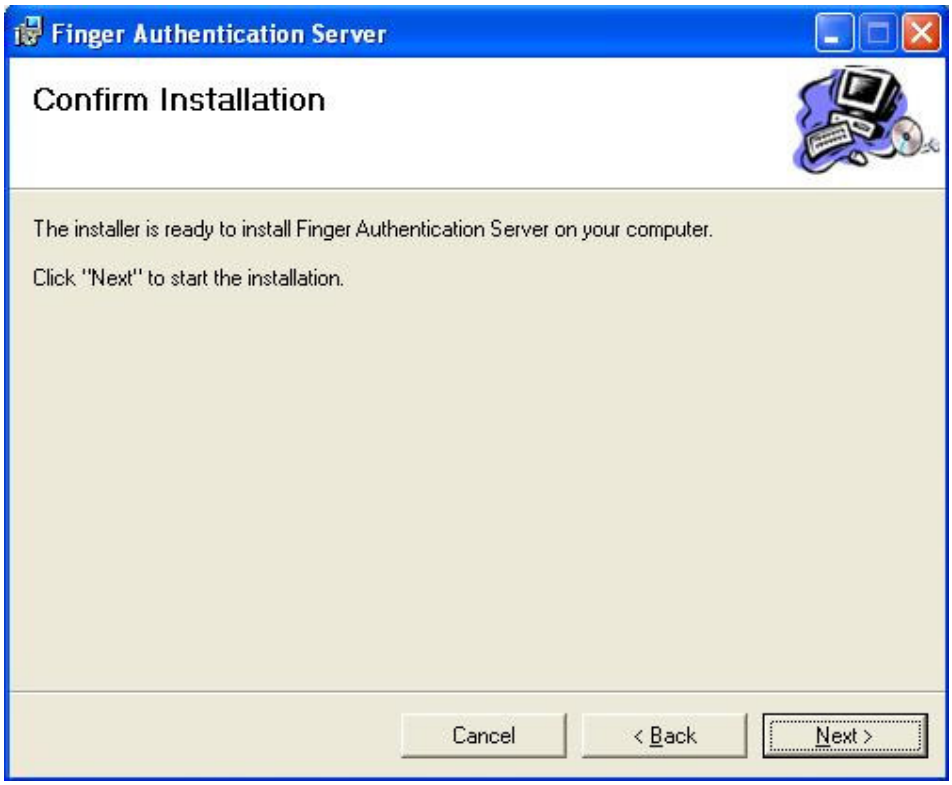
Please follow instructions of the installation wizard.

Click Next button to start the setup procedure.

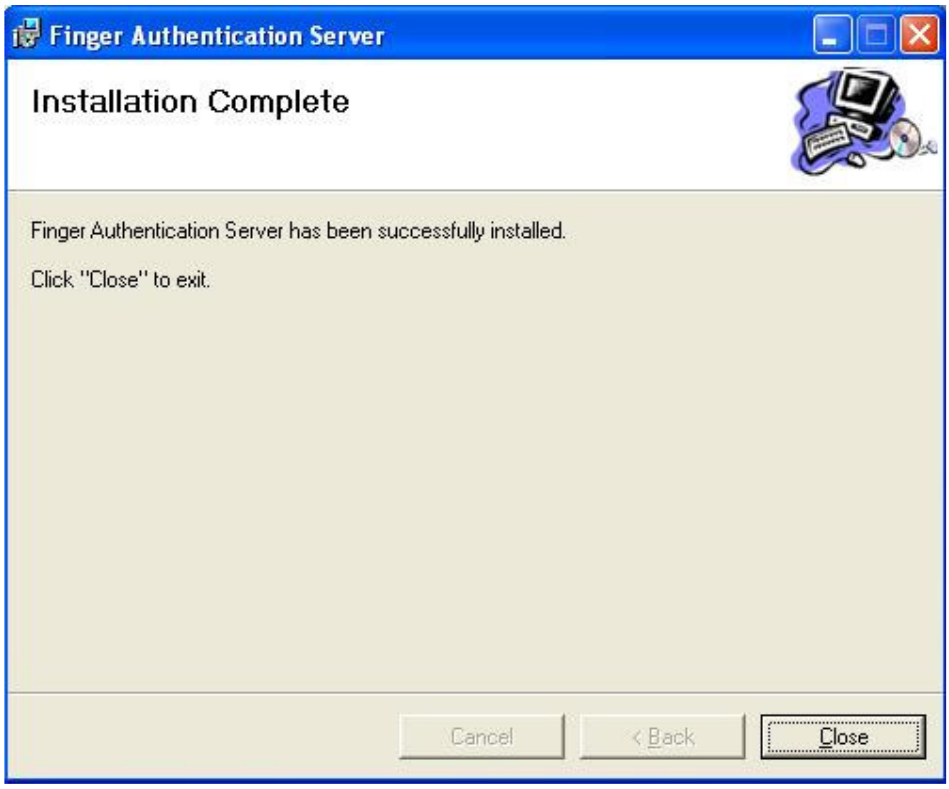
Select a folder where you want to install the program or just use the default folder.



Press “Next>” and the program will be installed on your computer.



Installation completed.

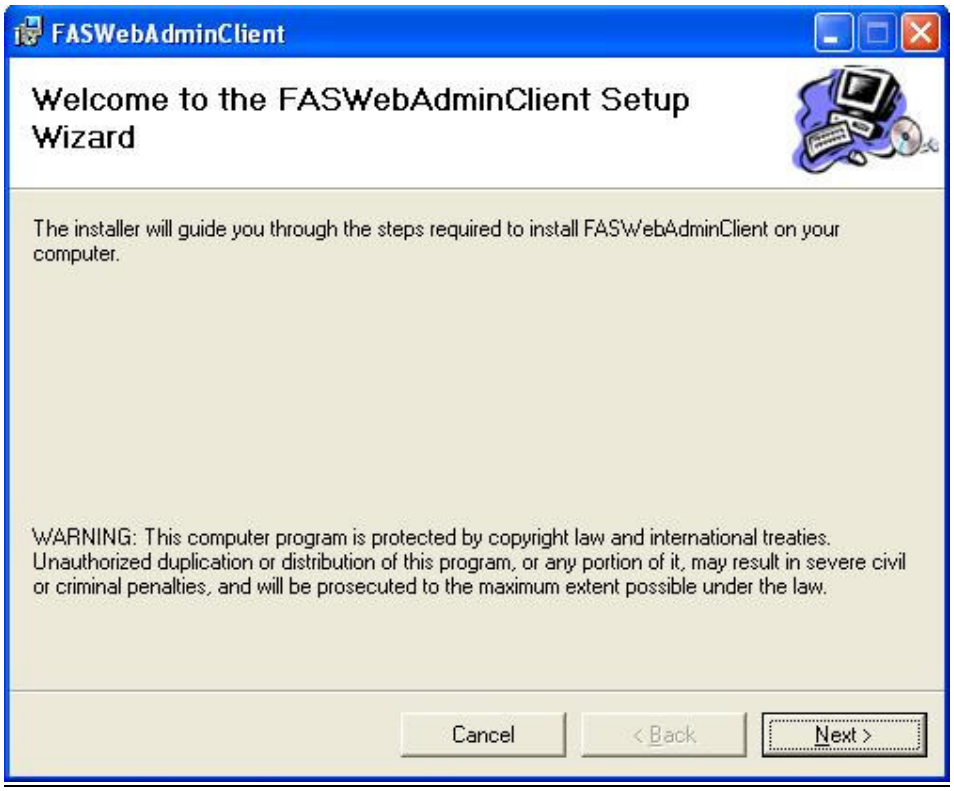


Click Close to exit.

2.4 Client Side Software – FASWebAdminClient

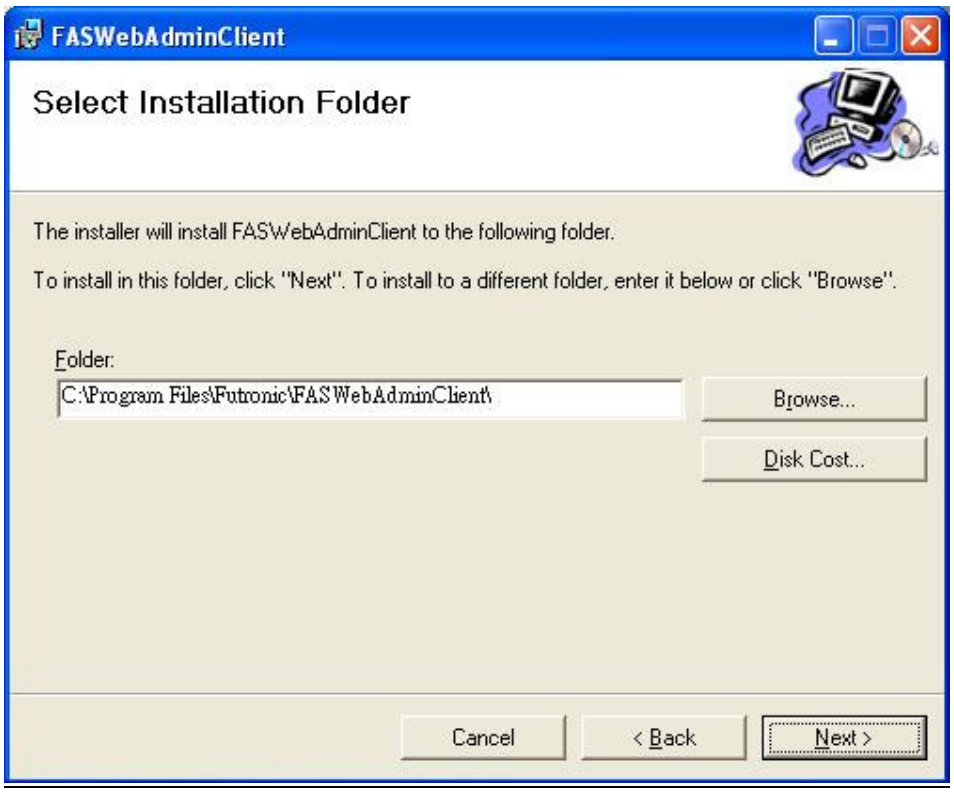
Client Side Software is installed in the pc, which is used to manage the FAS server through IE.

Please follow instructions of the installation wizard.

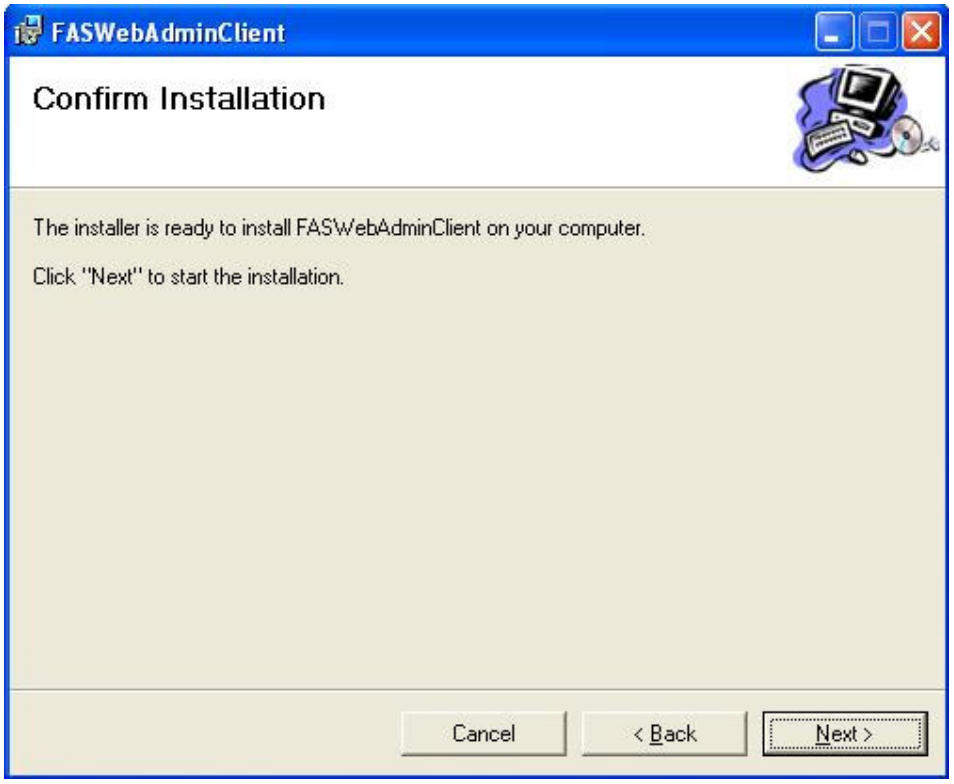


Click Next button to start the setup procedure.

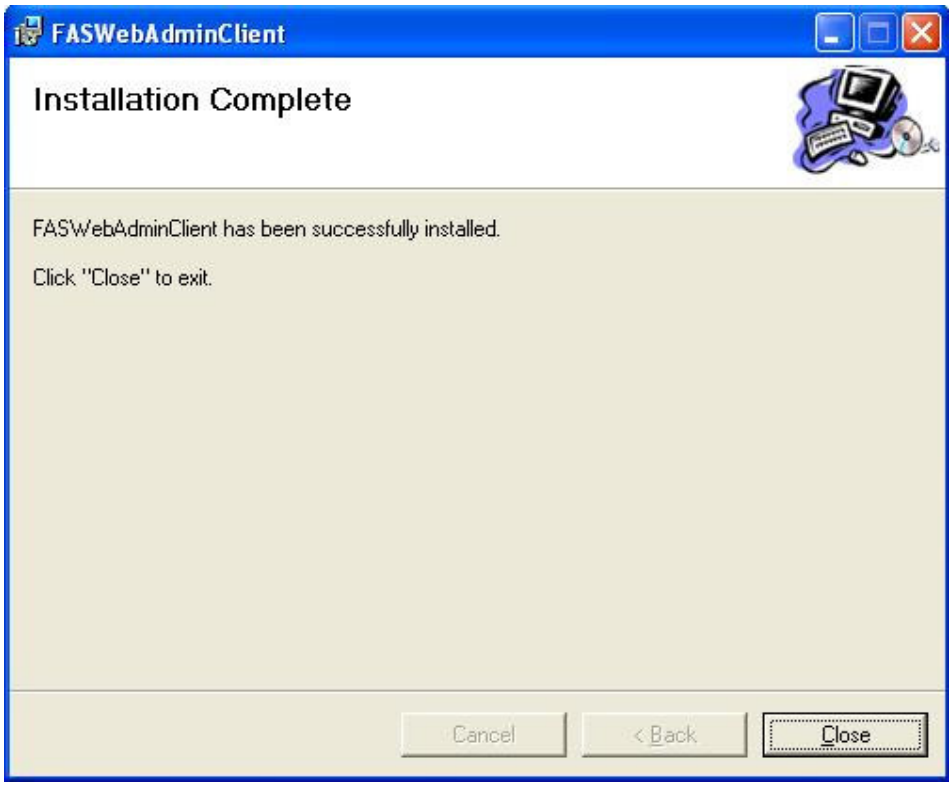
Select a folder where you want to install the program or just use the default folder.



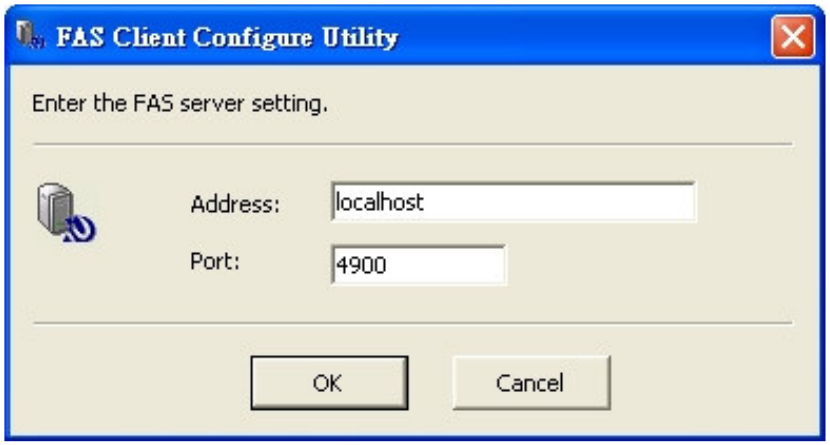
Press “Next>” and the program will be installed in your computer.



Installation completed.



In the popup window, input the address of FAS Server, it can be IP address or machine name of server. The default port number is 4900. Then click “OK” button.



Section 3. Un-installation

To remove the Server Side Software **Finger Authentication Server**, select the option Add/Remove Programs in the Windows control panel. Find **Finger Authentication Server** and press the "***Change/Remove"*** button.

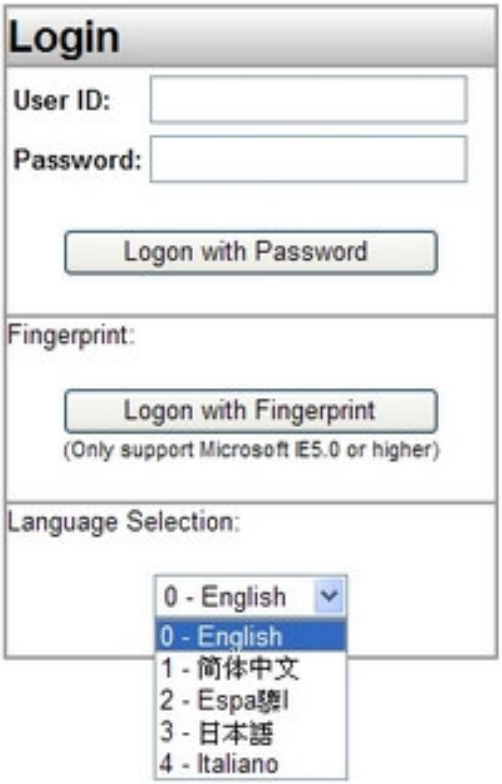
To remove the Client Side Software **FASWebAdminClient**, select the option Add/Remove Programs in the Windows control panel. Find **FASWebAdminClient** and press the "***Change/Remove"*** button.

Section 4. Getting Started

4.1 Administration

After installed the FASWebAdminClient software in the client PC, you can logon to the FAS from client PC through Microsoft Internet Explorer (IE).

Open IE, in the address field of IE, please input http://FASSERVER:4800, (FASSERVER is the machine name or IP address of the PC which installed FAS).



Now you can logon to FAS with password or fingerprint. The default administrator's user id is "**0**", password is "**welcome**". The first time you can just logon with password.

You can select the display language in the web pages. By default, there are 2 build-in languages, English and Simplified Chinese.

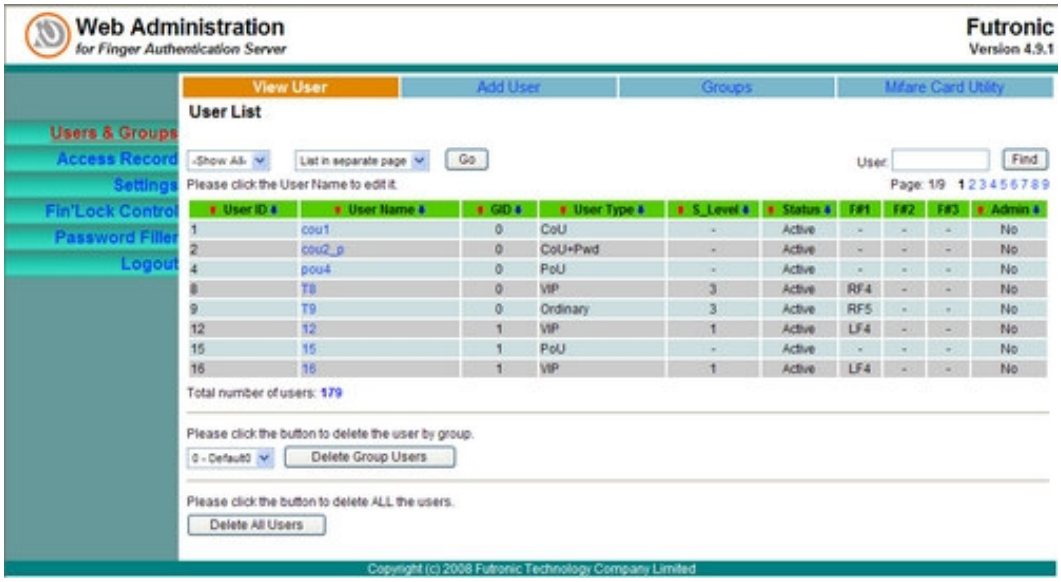
There are 6 sections in the web administration page, include: "**Users & Groups**", "**Access Record**", "**Settings**", "**Fin'Lock Control**", "**Password Filler**", "**Logout**".

4.2 Users & Groups

Users: Each user in the FAS has the following attributes:

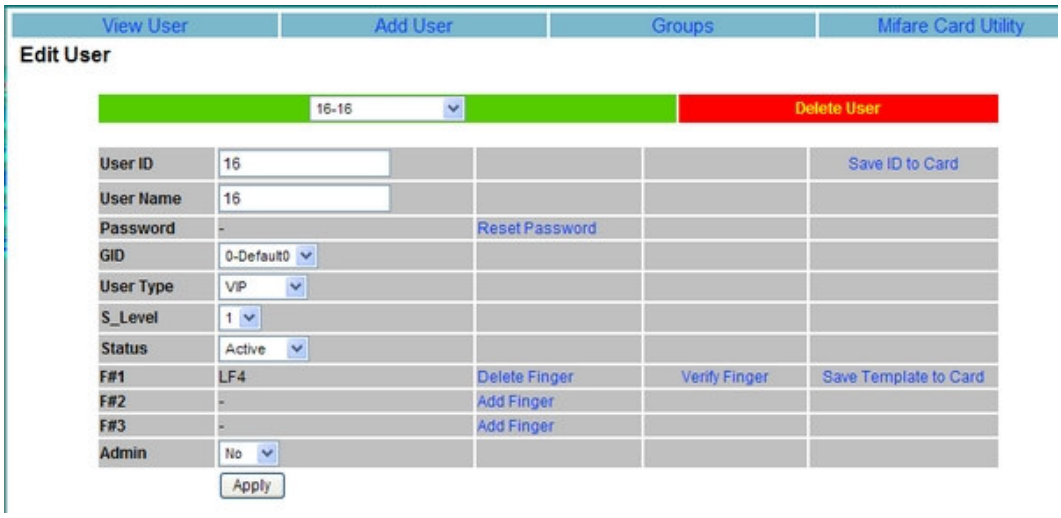
1. User ID: The unique ID for each user, can be up to 12 decimal digits (0-9)
2. Username: The real name of user
3. Password: The password for login to web page.
4. Group ID: Specify the group of a user belongs to. Value: 0-99.
5. User Type:
   - VIP: user just put finger to do 1-N matching;
   - Ordinary: user need to input the UID to do 1-1 matching;
   - CoU: Card Only User, just need the Mifare Card;
   - CoU+Pwd: Card Only User that need to type the password;
   - PoU: PIN Only User, need to input the user ID and the PIN.
6. Security Level: There are 4 security levels per-user, 1(lowest), 2, 3, 4(highest)
7. Status: Active or Suspend.
8. Fingerprint template: There are up to 3 fingers for each user.
9. Administrator: Yes or No. The administrator has the right to logon to FAS, enter all the admin pages, normal user just have the right to enter the page to view the access record.

Groups: Group is the collection of users with the same property, such as same department, same shift duty… Each user must belong to 1 group. Group is used to the section "In/Out Record" and "Permission".



4.2.1 View User

All the users are listed here. To edit each user, just click the username.



When you change any attribute, press the "Apply" button, and the attribute will be updated.

Each user can be added up to 3 fingers, in this page, you can "**Reset Password**", "**Add Finger**", "**Verify Finger**", "**Delete Finger**" and "**Delete User**".

If you have the FS25 device, you can also "**Save ID to Card**" and "**Save Template to Card**", it is the same as the function of FS21M, please refer to the user's guide of FS21M for details.

4.2.2 Add User

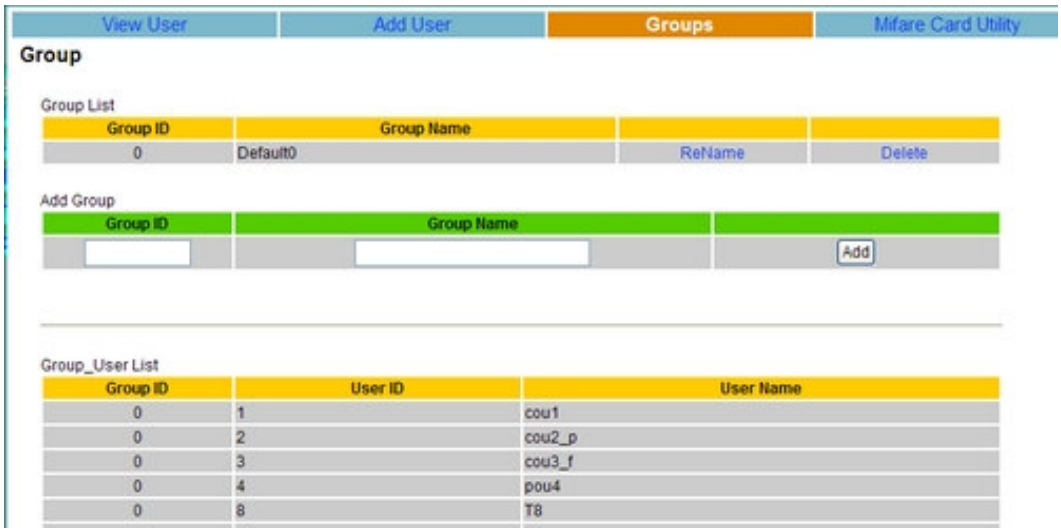
Add user to the FAS database.

User ID: the user id to assign to the user.
User Name: the real name of the user.
Password: the password for this user to login the FAS.
Finger: select the finger to be enrolled.
Finger Samples: you may select 1-5 fingerprint samples to be stored in the fingerprint template, 5 is the default value.
Admin: the user is an administrator or not.
Group: the user belongs to the group.
User Type:

- VIP: user needs not to input the user ID, just put the finger to do the 1-n matching.
- Ordinary: user needs to input the user ID and put the finger to do the 1-1 matching.
- PoU: Pin Only User. User need to input the user ID and password for verification.
- CoU: Card Only User. User just need the Mifare Card for verification, to add this user type, you need the FS25 device.
- CSN User: Card Serial Number user, user ID is the CSN, to add a CSN user, you need not to input the user ID, and it is detected by the FS25 device.

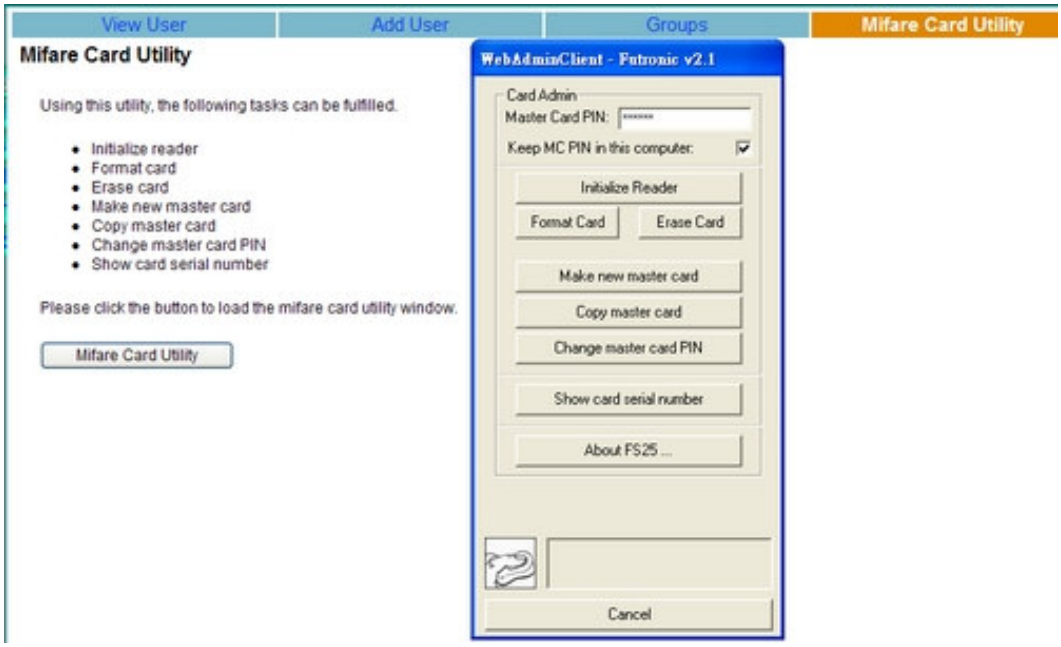
Security Level: it is used for VIP/Ordinary user.

4.2.3 Groups



All the groups and group users are listed here.
To add group, just input the Group ID and Group name, then press the "**Add**" button.
To delete a group, just click the related hyperlink "**Delete**".
To rename a group, just click the related hyperlink "**ReName**".

4.2.4 Mifare Card Utility



NOTE: This utility just work with the FS25 device ONLY.

Using this Mifare Card Utility, you can work with the FS25 device to do the following:

- Initialize reader
- Format card
- Erase card
- Make new master card
- Copy master card
- Change master card PIN
- Show card serial number

Please refer to the user's guide of FS21M for details.

4.3 Access Record

There are 4 types of user access log.

- Raw Access Log (RAL)
- Time Attendance Log (TAL).
- Denial Access Log (DAL)
- Alarm Log

Filter User ID or Name is used when the User ID or User Name is changed, but you want to show the old records for the User ID or Name before changing.

RAW Access Log (RAL)

RAL records all the access time of every valid user. Even more, it records the Finger ID of the user and the Fin'Lock ID.

- The RAL can be sorted by Group or User, and filtered by date, user id or name.
- The RAL can be sorted by Date Time
- The RAL can be exported to Text file and download to the client computer.
- The RAL can be exported to Excel file and download to the client computer.
- To delete the RAL records that you see in the page, just click the "Delete Current Record".
- To delete all the RAL records, just click the "Delete All RAW Access Log ", all the RAL records will be erased.
- To download the RAL records, click "Download Record", choose the file that you have exported, view it or download it.

Time Attendance Log (TAL)

TAL is generated from the RAL base on the TAL mode. There are 4 TAL modes for determining the In-time or Out-time.

1. First and Last in 24 hours: in a period of 24 hours, from 00:00 to 24:00, the first access time will be In-time, the last access time will be Out-time.
2. First in 24 hours: in a period of 24 hours, from 00:00 to 24:00, the first access time will be In-time, and the following access time will be discarded.
3. In/Out by sessions: Up to 12 sessions of each group can be defined to be "in", "out" or "don't care". The sessions are defined with the group ID.
4. In/Out by event: Up to 14 event IDs.

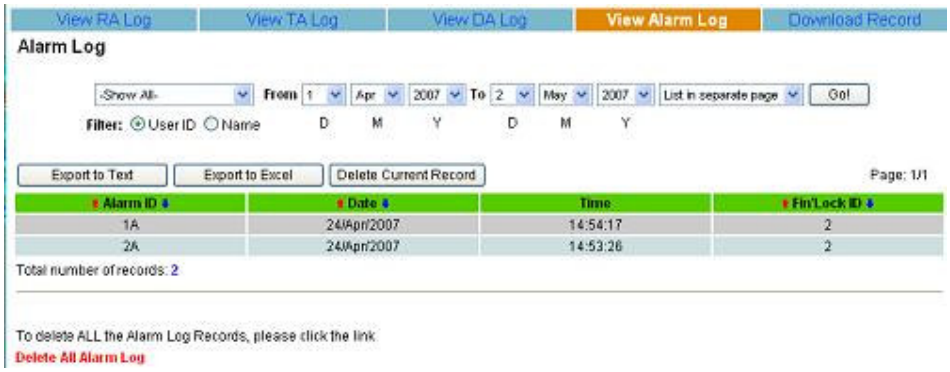
- The TAL can be sorted by Group or User, and filtered by date, user id or name.
- The TAL can be sorted by Date Time
- The TAL can be exported to Text file and download to the client computer.
- The TAL can be exported to Excel file and download to the client computer.
- To download the TAL records, click "Download Record", choose the file that you have exported, view it or download it.

Denial Access Log (DAL)

DAL records all the access time of invalid user, includes Suspend User and Denial User.

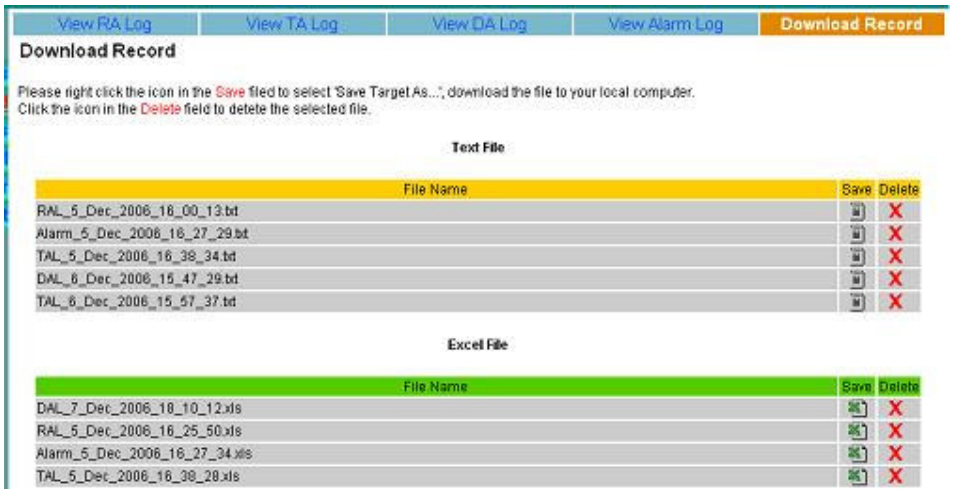
Alarm Log

Alarm log records the alarm event of the Fin'Lock.



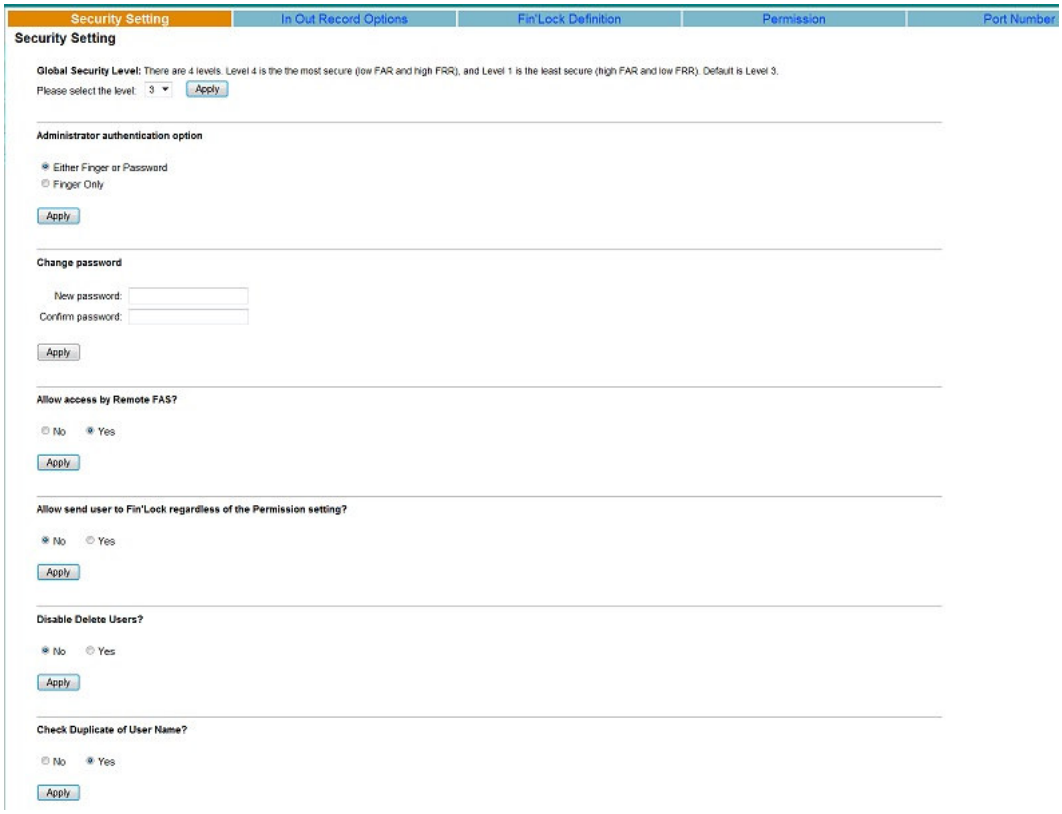
Download Record

All the access record which has been exported to text file or excel file can be downloaded to the client pc. It can also be deleted from the FAS.



4.4 Settings

Basic setting of FAS.



4.4.1 Security Setting

1. Global Security Level: there are 4 security levels, 1(lowest), 2, 3, 4(highest). To change the level, just select the level and press the button “Apply”.
2. Administrator Authentication Option: there are 2 options, “Finger Only” is the highest security.
3. Change administrator password: To change the administrator password, just input the new password twice, then press “Apply”.
4. Allow access by remote FAS: If “Yes”, the FAS can be accessed by other remote FAS, and works as a Fin’Lock. For security, do NOT set it to “Yes” unless you know what you are doing.
5. Allow send user to Fin’Lock regardless of the Permission setting: When sending user to the Fin’Lock from the menu “FinLock Control->Send User”, the Permission setting will be checked. To disable the checking, you can choose the option “Yes”.
6. Disable Delete Users: If “Yes”, the links in the “Users and Groups” to delete user will be hidden. The default is “No”.
7. Check Duplicate of User Name: If “No”, the user name can be duplicated. The default is “Yes”.

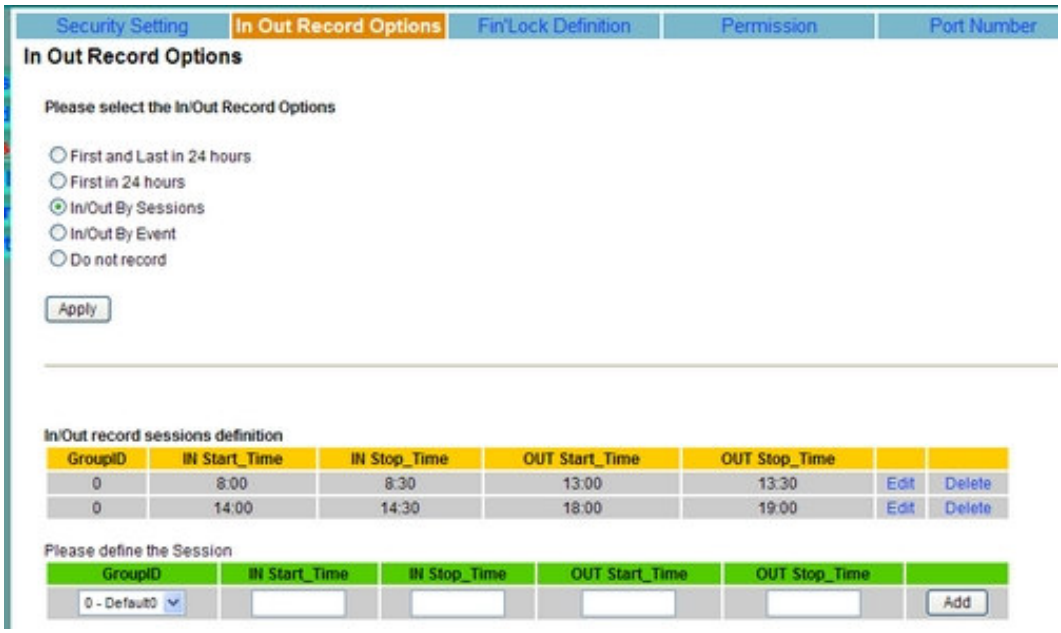
4.4.2 In Out Record Options

There are 5 options:

1. First and Last in 24 hours
2. First in 24 hours
3. In/Out By Sessions
4. In/Out By Event
5. Do not record

To change the option, just select the option and press “Apply”.
The TAL is generated from RAL according to this option.

For option 3, it is necessary to define the In/Out Sessions. Select Group ID, then input the time periods of IN and OUT session, from start to stop, press “Add”. The TAL is generated from RAL according to the predefined sessions.



For option 4, the raw access log (RAL) is recorded according to the **Event Settings in the Fin’Lock**, The event ID will be kept in the field InOutOption of table [RALog]**.** The event setting can be set in FAS and then send to Fin’Lock, or set in the Fin’Lock and then get from the Fin’Lock to FAS.

If you set it to option 5, the raw access log (RAL) will NOT be recorded to the FAS.

4.4.3 Fin'Lock Definition

Every Fin'Lock must have one unique ID. To add the definition, please input the Fin'Lock ID, Fin'Lock IP and Description, then press the button "Add" to define the Fin'Lock.

IMPORTANT: Once you added a Fin'Lock, please turn on the 'Allow init' in Fin'Lock menu and then click the related hyperlink **'Initialize'** to set up the connection between Fin'Lock and FAS. It just need to do only **ONCE**.

You can install more than one FAS, and define remote FAS to communicate between them in the page "FinLock Control". For example:

In FAS-1: a. Define the remote FAS-2
b. Set "Allow access by Remote FAS" in the "Security Setting" to "Yes".
In FAS-2: a. Define the remote FAS-1
b. Set "Allow access by Remote FAS" in the "Security Setting" to "Yes".
c. Click "Initialize" to initialize the both FAS.

4.4.4 Permission

By default, all groups and users are allowed to access all Fin'Lock at all time.

To prevent the user to access from one Fin'Lock at some time, just add the user to the denial setting.

To prevent the group users to access from one Fin'Lock at some time, just add the Group ID to the denial setting.

You can define the permission by Date/Time or Weekday/Time.

Notes for **Date/Time** definitions:

- If the **From_Date** and **To_Date** are empty, it means every day.
- If the **From_Date** is empty, it means from anytime to "To Date/Time".
- If the **To_Date** is empty, it means from "From Date/Time" to forever.

After the permission is added, you can delete, edit or disable it by click the related hyperlink.

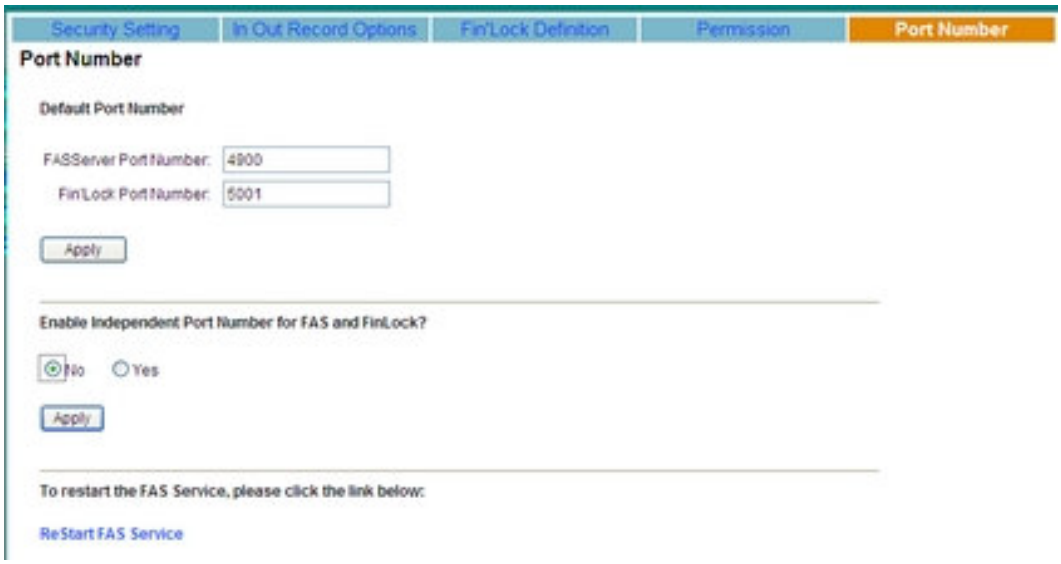
4.4.5 Port Number

By default, the FAS is listening to the port number 4900. Fin'Lock is listening to the port number 5001.

To change the port number, input the new port number (1-65536), and press the button "Apply".

If the FAS port number is changed, it is necessary to restart the FAS, just click the hyperlink "ReStart FAS Service" to restart the FAS.

If you change the setting, please change the setting in the Fin'Lock accordingly.



The option "Enable independent port number for FAS and Fin'Lock" is a new option added in FAS v5.5, by default it is set to "No", if it is set to "Yes", the page of "Fin'Lock Definition" will be changed as below:

This option is useful for FAS and Fin'Lock to work on the Internet environment, you can set a fixed real IP for FAS and a fixed real IP for Fin'Lock, the FAS and Fin'Lock can be the virtual IP of the LAN behind a router, and the function of "Port Forwarding" in the router is added according to the port number. Using this option, you can set multiple Fin'Locks in one LAN with the only one same real IP.

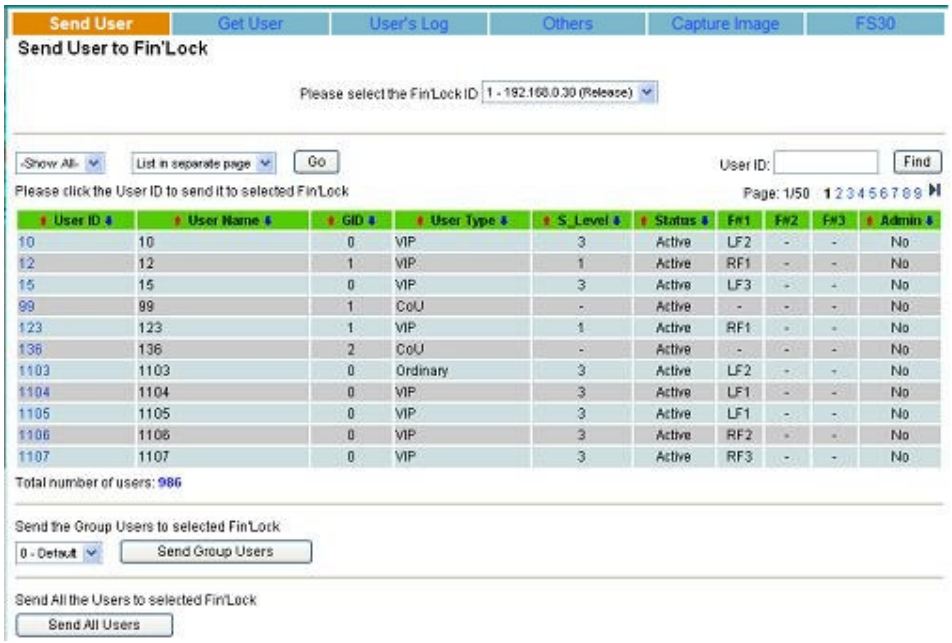
NOTE: If your Windows OS installed the third party firewall software, please allow the TCP Port 4900 and 4800, or the FAS could not work properly.

4.5 Fin'Lock Control

This section includes the commands to control the Fin'Lock and Remote FAS through TCP/IP network, the Remote FAS can be controlled just as Fin'Lock device.

4.5.1 Send User

Send the users of FAS to Fin'Lock or remote FAS. All the attributes of this user will be sent to selected Fin'Lock, except for the attribute "Username" and "Admin". All the attributes will be sent to remote FAS.



All the users of FAS are listed here. There are 3 ways to send user to Fin'Lock,

1. Send individual user to Fin'Lock, click the "User ID" to do it.
2. Send group users to Fin'Lock, please select the Group, then press the button "Send Group User", all the users belong to this group will be sent to the selected Fin'Lock.
3. Send all the users to Fin'Lock, just press the button "Send All Users".

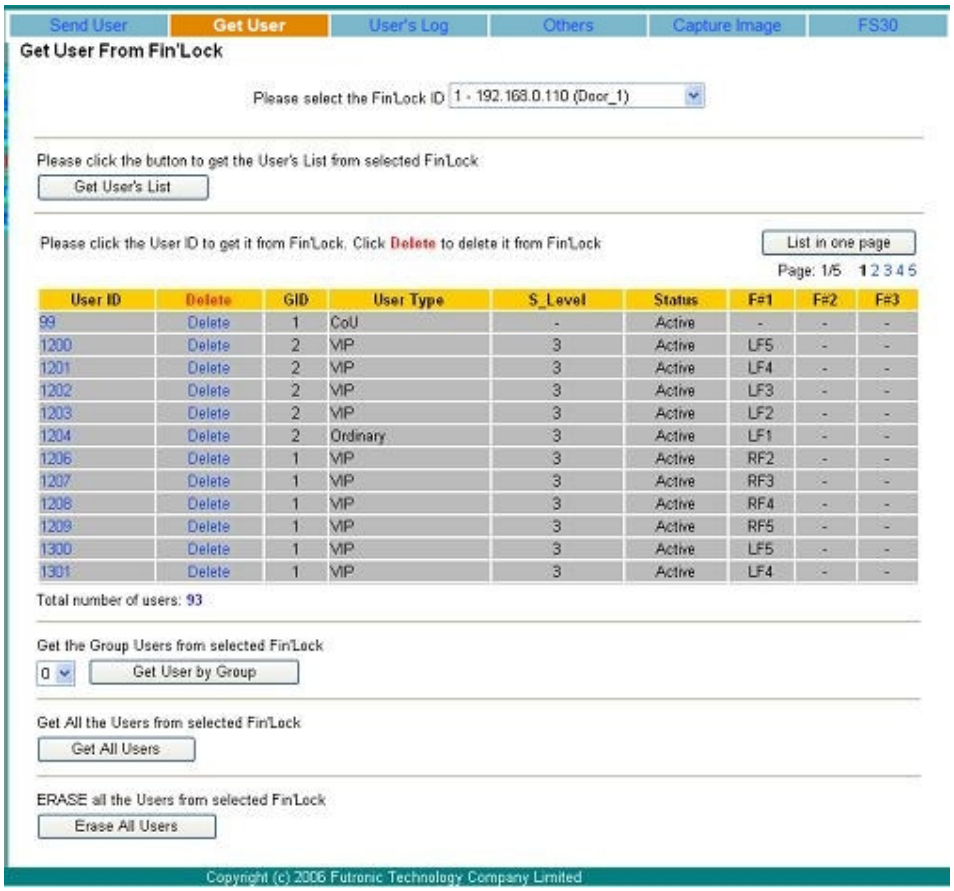
NOTE: If the User ID existed in the Fin'Lock, all the user data will be erased and replaced with the new one.

4.5.2 Get User

To get the users from Fin'Lock to FAS, please select the Fin'Lock from the top of this page, then press the button "Get User's List", all the users of this Fin'Lock will be listed here. There are 3 ways to get the user from Fin'Lock to FAS.

1. Get individual user from Fin'Lock, click the "User ID" to do it.
2. Get group users from Fin'Lock, please select the group, then press the button "Get User By Group", all the users belong to this group will be got from Fin'Lock.

3. Get all the users from Fin'Lock, just press the button "Get All Users".



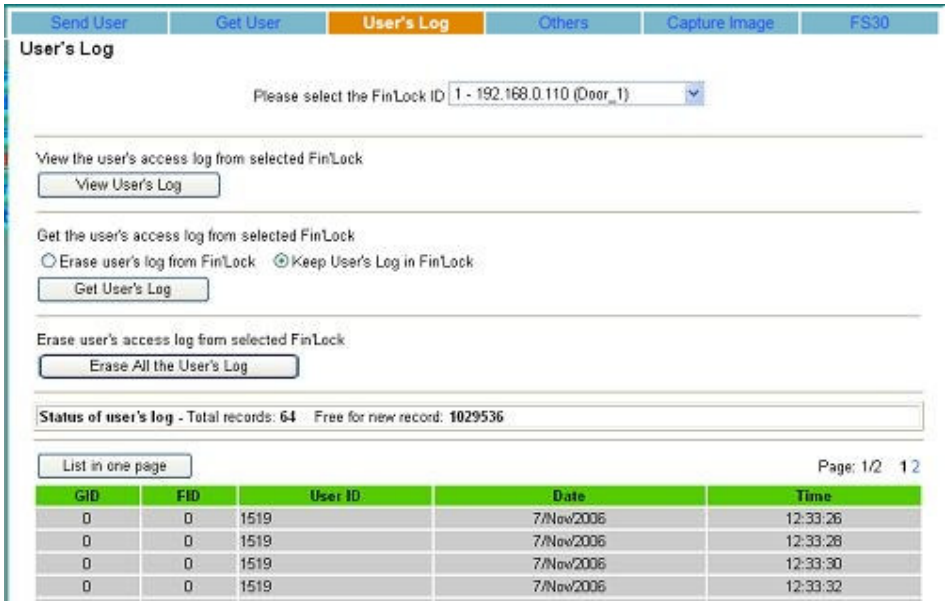
To delete the user in selected Fin'Lock, just click the related "Delete", and the user will be erased from the Fin'Lock.

To delete all the users in Fin'Lock, just press the button "Erase All the Users". All the user data will be erased from the selected Fin'Lock.

NOTE: If the User ID existed in the FAS, all of the user data will be erased and replaced with the new one got from Fin'Lock.

4.5.3 User's Log

Fin'Lock can run on 2 operation modes, Network or Local. If Fin'Lock runs on Local Mode or if the network connection is broken, the user access log will be kept in the Fin'Lock.



To check the user's log in Fin'Lock, just select the Fin'Lock and press the button "View User's Log", the user's log number and free for new log number will be listed below.

To download the user's log from Fin'Lock to FAS, select the Fin'Lock and press the button "Get User's Log", all the user's log will be downloaded from Fin'Lock to FAS and add to the database of FAS. There are 2 options during this operation, "Erase user's log from Fin'Lock" and "Keep user's log in Fin'Lock", if you select "Erase user's log from Fin'Lock", after the log is downloaded, the log will be erased from Fin'Lock.

To erase all the user's log in Fin'Lock, select the Fin'Lock at the top of this page and press the button "Erase All the User's Log".

4.5.4 Others

Other useful commands.

Get Information: The information include BF Firmware version, AVR Firmware version, Hardware version, Number of free pages, Global security level.

Set Security Level: There are 4 security levels in Fin'Lock, to set the global security level, select the level and press the button "Set Security Level".

Synchronize Time: Set the time of the Fin'Lock the same as FAS.

Open Door #x: Open the door relay control of Fin'Lock #x.

Set the schedule to synchronize time between FAS and Fin'Lock.(for all Fin'Locks)**:** This option let you to set the schedule to synchronize time between FAS and Fin'Lock automatically. It has the following options: Every 0 – Disabled, 1, 2, …, 24 Hour.

NOTE: The schedule to synchronize time does NOT synchronize the time of other FAS.

4.5.5 Capture Image

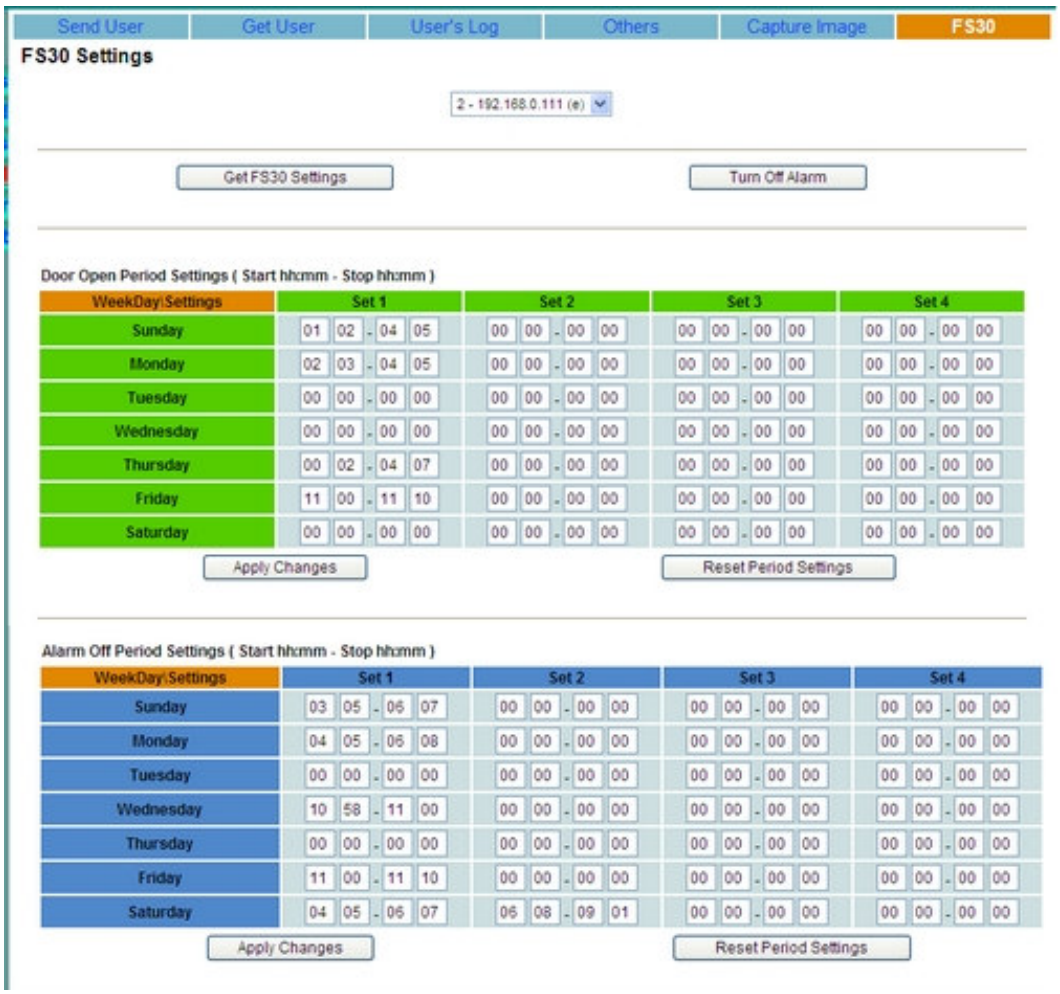
To detect the quality of fingerprint image in Fin'Lock, you can send the fingerprint image from Fin'Lock to FAS, then view it or download it from FAS to the client computer. This function is useful for troubleshooting.

4.5.6 FS30

This page is added in FAS v5.5, it is used to get/set the “Door Open Period” and “Alarm Off Period” settings from/to Fin’Lock, and turn off the FS30 alarm manually.

- Get FS30 Setting: Get the “Door open period” and “Alarm off period” settings in Fin’Lock.
- Turn Off Alarm: Turn off the alarm of FS30
- Apply Changes: If you change the setting, press this button to make the change to Fin’Lock.
- Reset Period Settings: Reset all the settings in Fin’Lock to 0.

Please refer to the Fin’Lock user’s guide for details.



4.6 Password Filler

Only Samba Logon is supported at this moment.

To use this function, you need to install another software “FinLogon FAS Client”. Install the software in the client computer, associated with FAS, you can use the registered users and fingers in FAS to logon your Samba server.

4.6.1 Profile

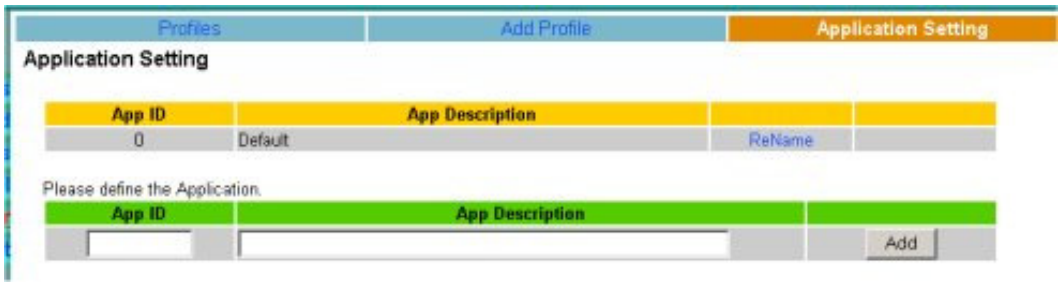
This page shows the registered Samba user in FAS. Please click the user name to edit the profile.

In this page, you can change the Samba logon name, logon password, status, even delete it.

4.6.2 Add Profile

In this page, you can add a new profile, please select the User ID in FAS according to the Samba user, input the username and password, click the button to add the profile.

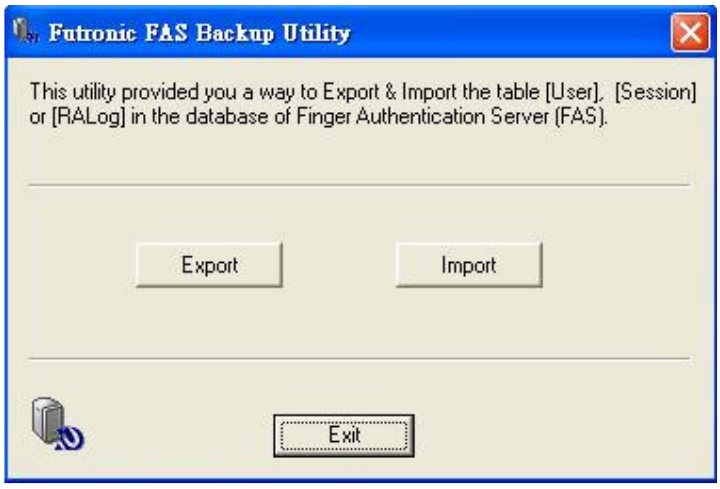
4.6.3 Application Setting



NOTE: Only Samba Logon is supported at this moment, please ignore this page.

Section 5. FAS Backup Utility

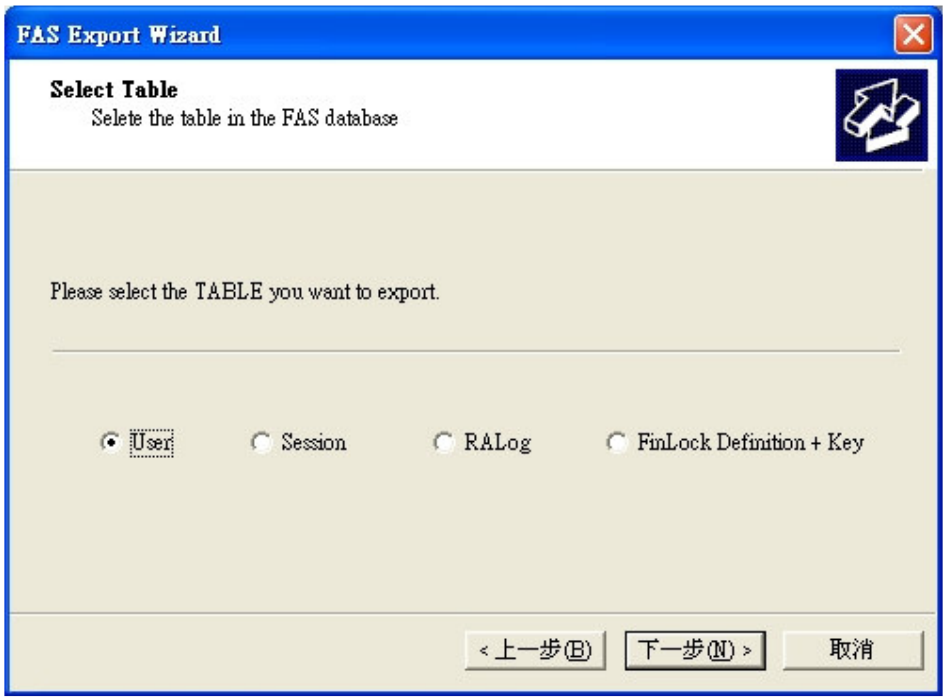
After installed the FAS, the FAS Backup Utility will be installed to the FAS Server. The shortcut is located in the menu ***Start->Programs->Futronic->FAS Backup Utility***. It provided a way for the administrator to backup the data of table [User], [RALog], [Session] and [FacDefinition] in the database of FAS.



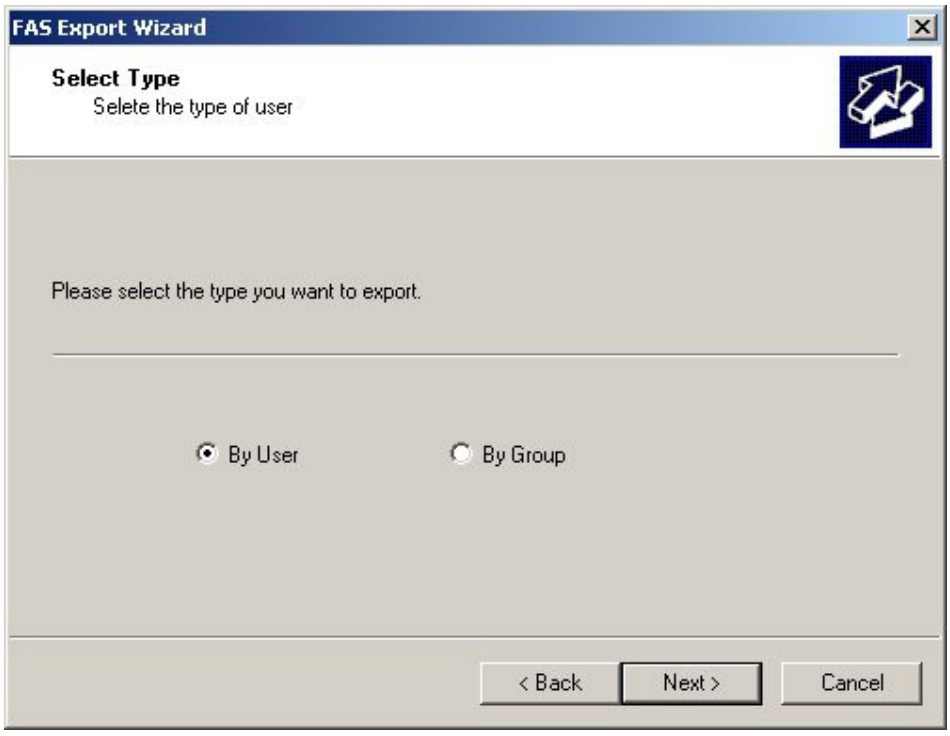
5.1 Export

To export the data of Users or Sessions to a file, please press the button “Export”. With the help of the export wizard, it is an easy job.

Click the “Next” button to begin.

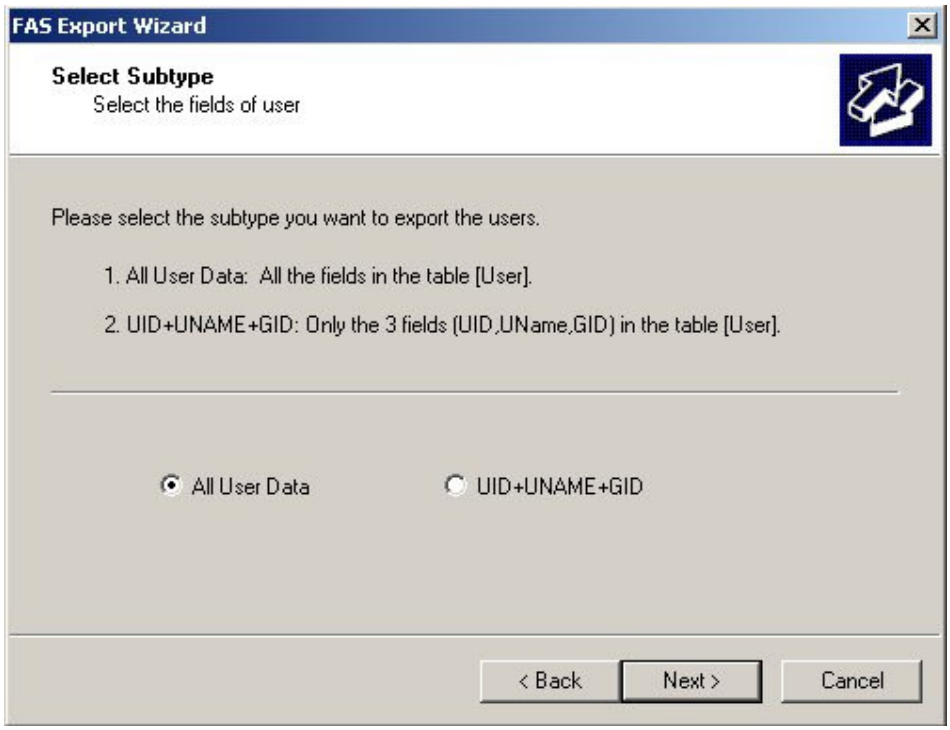


Select the table you want to export and then click “Next” button.

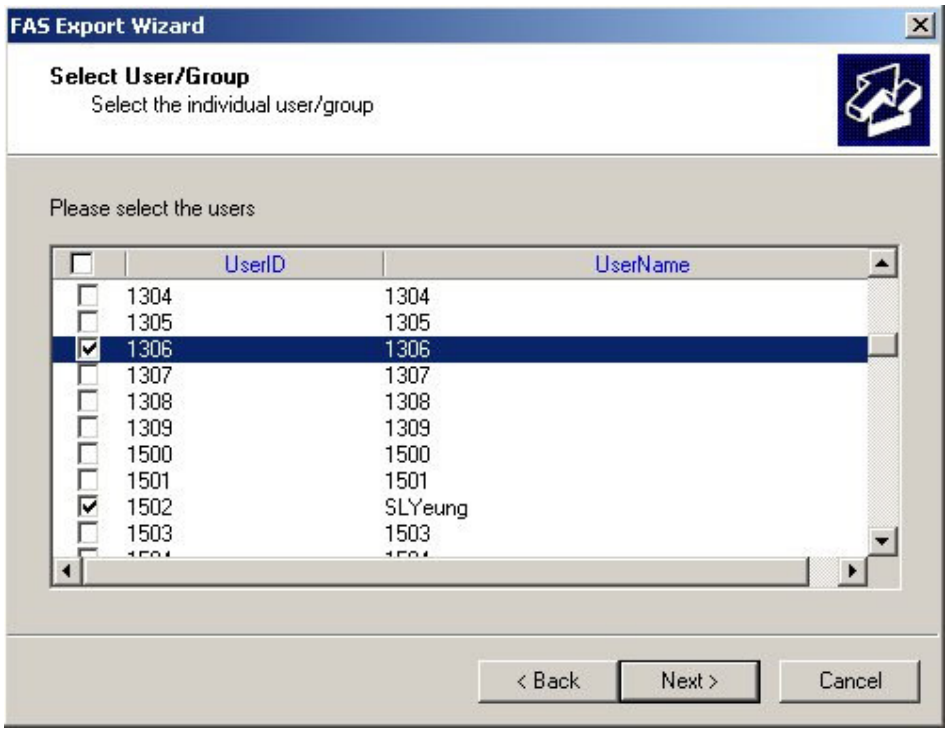


The User data can be exported by user or by group, and you can choose to export all the user data (with fingerprint template) or just the 3 fields (GID+UID+UNAME).

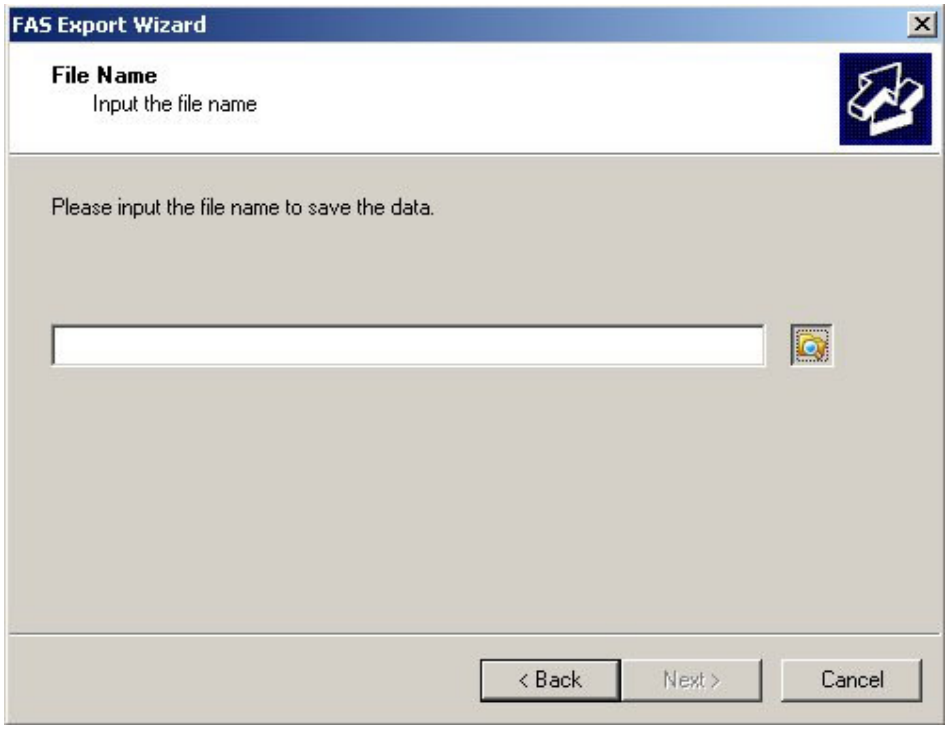
If you choose to export the 3 fields, you can export it to an Excel(.xls) or Text(.txt) file.



Please check the user you want to export and click “Next” button.



Please click the “Browse” button to input the path and file name to save the data. Then click the “Next” button.



After the data is exported, please click the “View Log” button to view the log, click the “Finish” button to close the export wizard.

To export the [Session], please follow the same wizard steps. You can export it to an Excel(.xls) or Text(.txt) file.

To export the [RALog] and [Session], please follow the same wizard steps.

If the Fin'Lock has been defined and initialized, there is a Key generated in FAS to communicate with that Fin'Lock. To export the Fin'Lock Definition and the related Key, please follow the same wizard steps.

5.2 Import

To import the data of Users or Sessions from a file, please press the button "Import". With the help of the import wizard, it is an easy job.

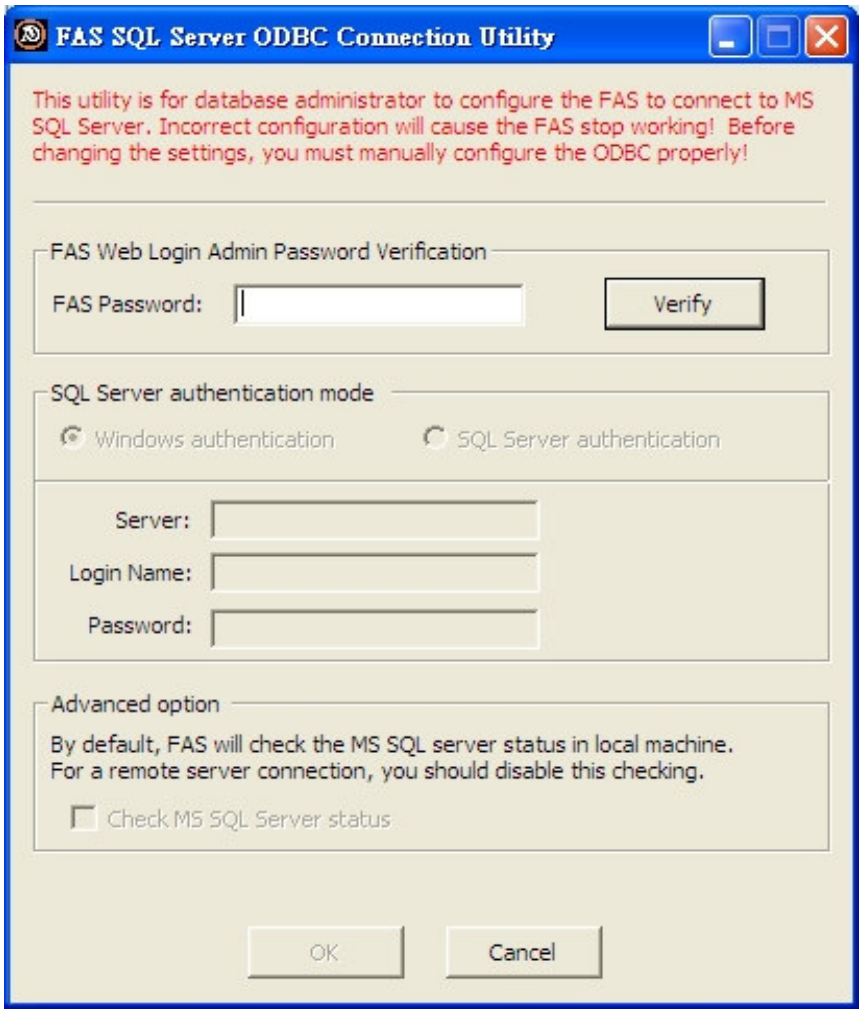
Please follow the wizard steps to finish the "Import" task.

Notes:

1. If the UID exists in the FAS, it will be **SKIPPED** during the importing.
2. If the Session exists in the FAS, it will be **ERASED** during the importing.
3. If the access log exists in the FAS, it will be **SKIPPED** during the importing.
4. If the Fin'Lock definition and the Keys exist in the FAS, it will be **ERASED** during the importing.

Section 6. FAS SQL Server ODBC Connection Utility

This utility is used for database administrator to configure the FAS to connect to MS SQL Server.



By default, the FAS database is installed to the local system with Windows Authentication Mode, and this utility is not needed to use. But if you want to setup the FAS database "FASSQL" to other PC, and/or uses SQL Server Authentication mode, you can use this utility to change the settings for FAS.

1. Install the database "FASSQL" as you needed.
2. Configure the ODBC system source name "FtrFas" accordingly.
3. Run this utility and click "OK" to re-start the FAS services.

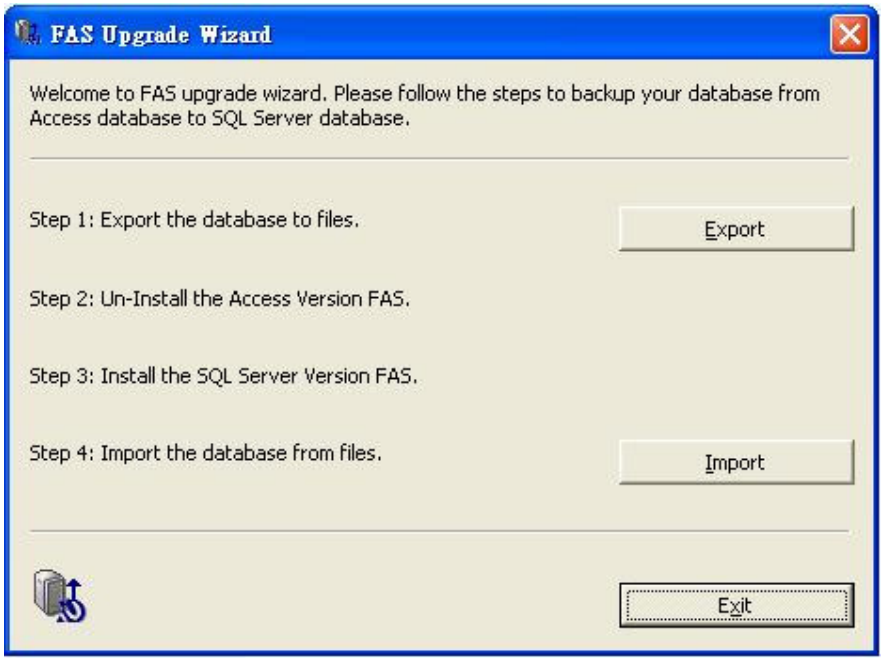
Section 7. Upgrade

There is not an upgrade option in the setup script, to upgrade from the old version FAS (version 3.0 or earlier), you need to un-install the old version FAS and then install this version FAS (version 4.0 or later).

We provided a utility (FASUpgradeWizard.exe) to let you export all the data from the MS Access database in the old version FAS, and import to the MS SQL server database in this version FAS.

IMPORTANT: Before you un-install the old version FAS, please run this utility to export the data.

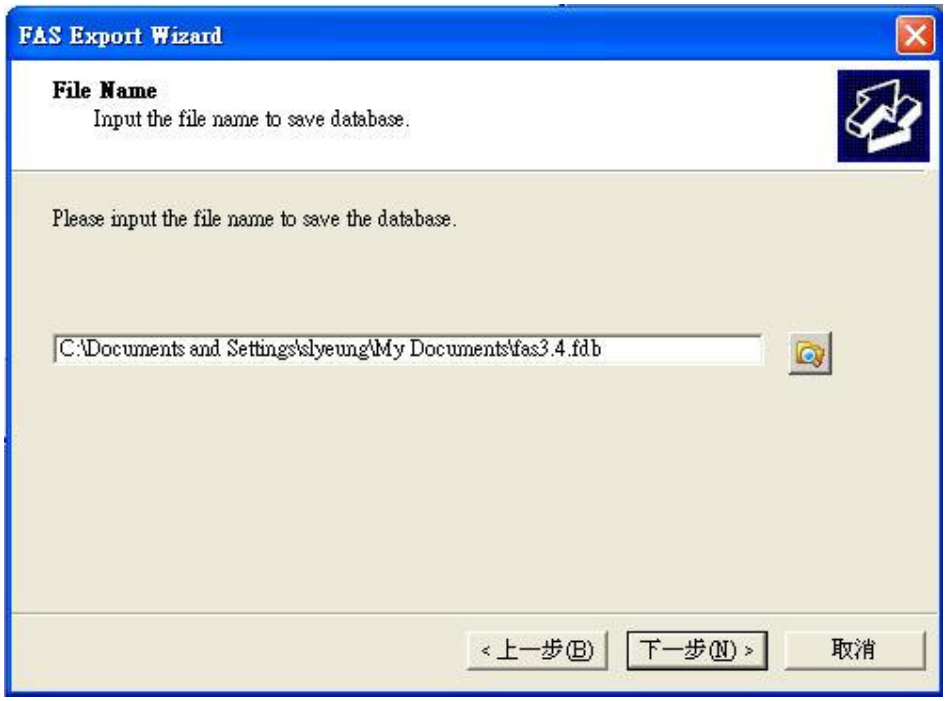
Please follow the steps to migrate the data.



6.1 Export

Please press the button “Export” to begin to export the data to a file.

Click “Next >” to continue.



Click the “Browse” ICON button to select the folder and input a file name, then click “Next >” to continue.

All the data will be saved to the file you just input. Click “Finish” to close the wizard.

6.2 Import

After you un-install the old version FAS and then install the new version FAS, you can import all the data from the file you just saved in 6.1.

Please press the button “Import” to begin the import wizard. The procedure is the same as Export.