MagicSecure 3.0
FINGERPRINT IDENTIFICATION

User's Guide

FCC Information

This equipment has been tested and found to comply with limits for a class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.
This equipment can generates, uses, and radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio Communications. However, there is no guarantee that interference will not occur in a particular Installation.
If this equipment does cause unacceptable interference to radio and television reception, which
can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures.

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the Receiver is connected.
- Consult the dealer or an experienced Radio/TV technician for help.

Caution : Any changes or modifications in construction of this device which are not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

IMMANUEL
IMMANUEL ELECTRONICS CO.,LTD.

Introduction to Ramses II

Ramsen II is an innovative PC security product developed by Immanuel Electronics Co., Ltd. for providing security and a means of authentication to its users.
Ramses II fingerprint identification capability will enable you to implement a convenient and solid security system.

Your fingerprint is the most convenient and safest key.

You no longer have to worry about losing your password.
Also, no more worries about others knowing your password.
You don't have to know anything about complex encryption algorithms.
Ramses II will protect your system with your fingerprint as the key to security.

Ramses II the logon procedure, provides screen saver security and protects your files and folders.

Ramses II features fingerprint authentication logon,
screen saver security and file/folder protection. These features protect your system not only when it is turned on and off,
but also when you momentarily leave your system.
Furthermore, it enables you to select the identification scheme (fingerprint/password) and provides various administrator functions.

Ramses II is an outstanding software product

Ramses II received the **2000 New Software Grand Prize**
and the **Chairman's Award at SOFT EXOP 2000.**
It has been widely recognized as an innovative and
reliable software product.

Applications

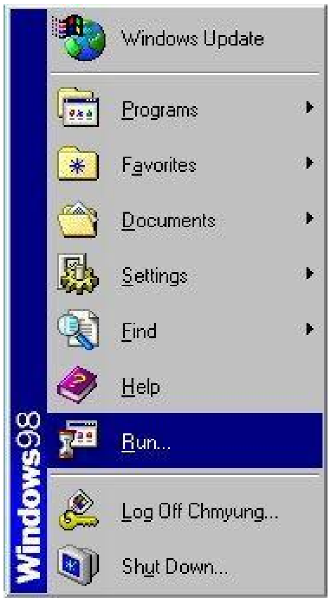
- Personal authentication and identification for electronic financial transactions, e-mails and electronic document exchanges
- Personal system security for protecting system data
- System access restriction and data protection
- Security and authentication measures for Internet and e-commerce applications

System Requirements

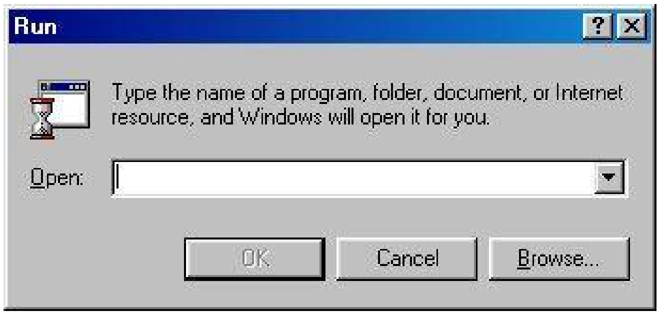
- OS: Microsoft Windows 98, Microsoft Windows 98SE, Microsoft Windows ME
    - CPU: Pentium 133MHz or greater
    - HDD: Free disk space of 20MB or more
    - Memory: 32 MB or more
    - Device: Ramses II Fingerprint Scanner/Mouse
    - Required Program: Microsoft Internet Explorer 5.0 or later

Chapter 1. Program Installation

Insert Ramses II CD in your CD-ROM drive and run setup.exe to install Ramses II



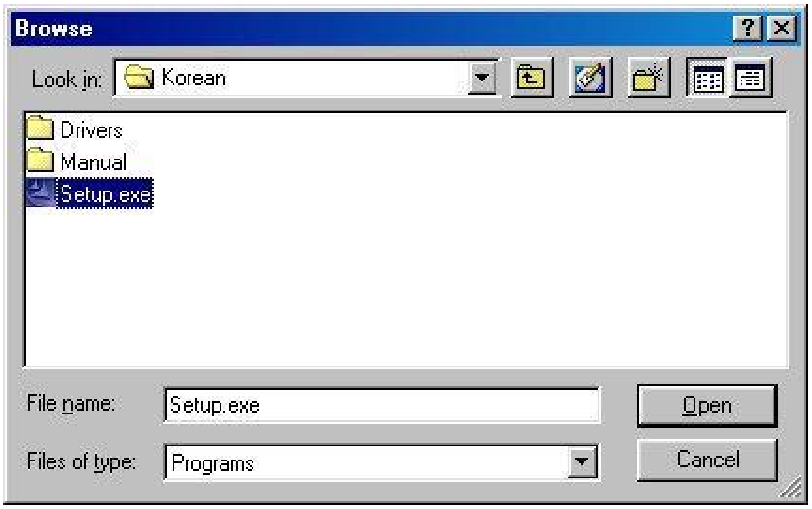
Select **Start > Run** from the taskbar.


Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open:

Input the file path in the **Open** text box
or click **Browse…** and specify the path.



Browse

Look in: Korean

Drivers

Manual

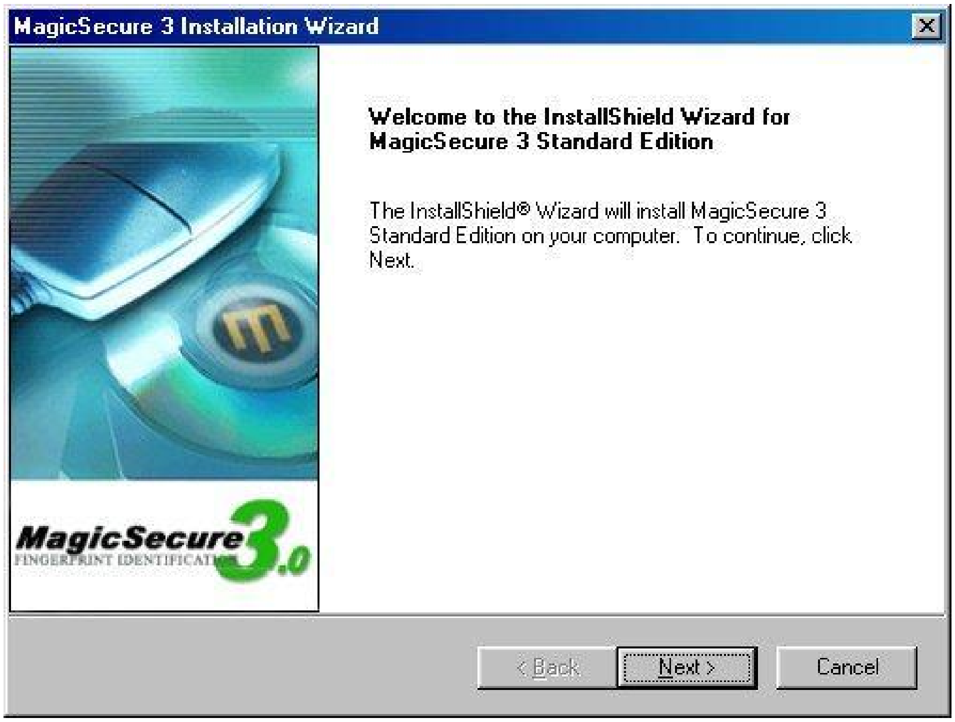
Setup.exe

File name: Setup.exe

Files of type: Programs

From the **Browse** window, select "setup.exe" and click **Open**.

The file path will be indicated in the **Run** window. Click **OK**.

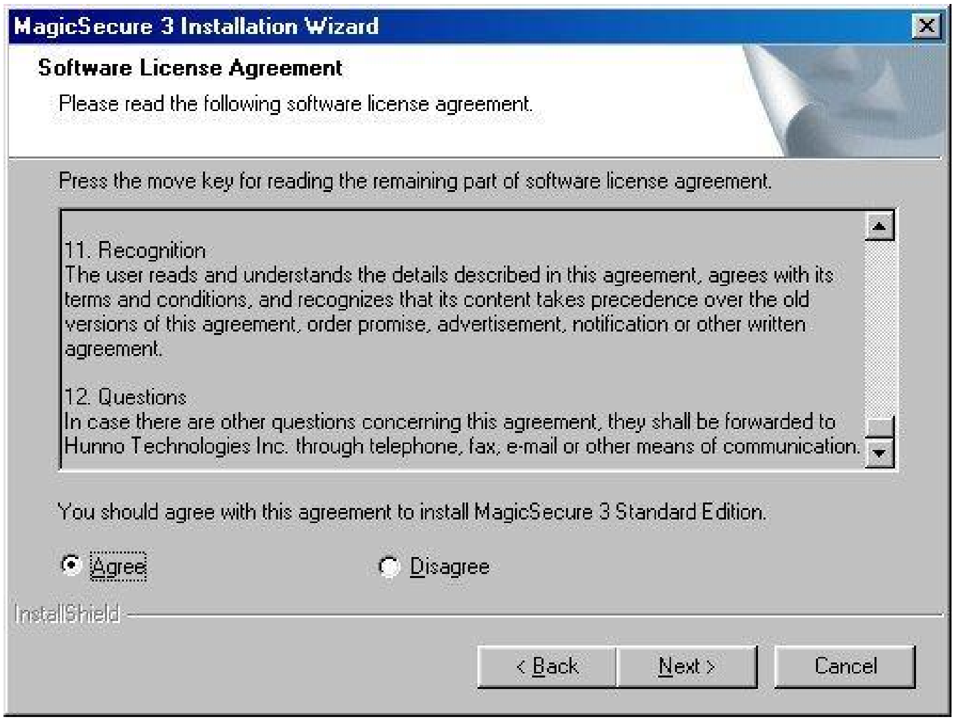


MagicSecure 3 Installation Wizard

Welcome to the InstallShield Wizard for MagicSecure 3 Standard Edition

The InstallShield® Wizard will install MagicSecure 3 Standard Edition on your computer. To continue, click Next.

The initial screen for program installation will be displayed. Click **Next**.



MagicSecure 3 Installation Wizard

Software License Agreement

Please read the following software license agreement.

Press the move key for reading the remaining part of software license agreement.

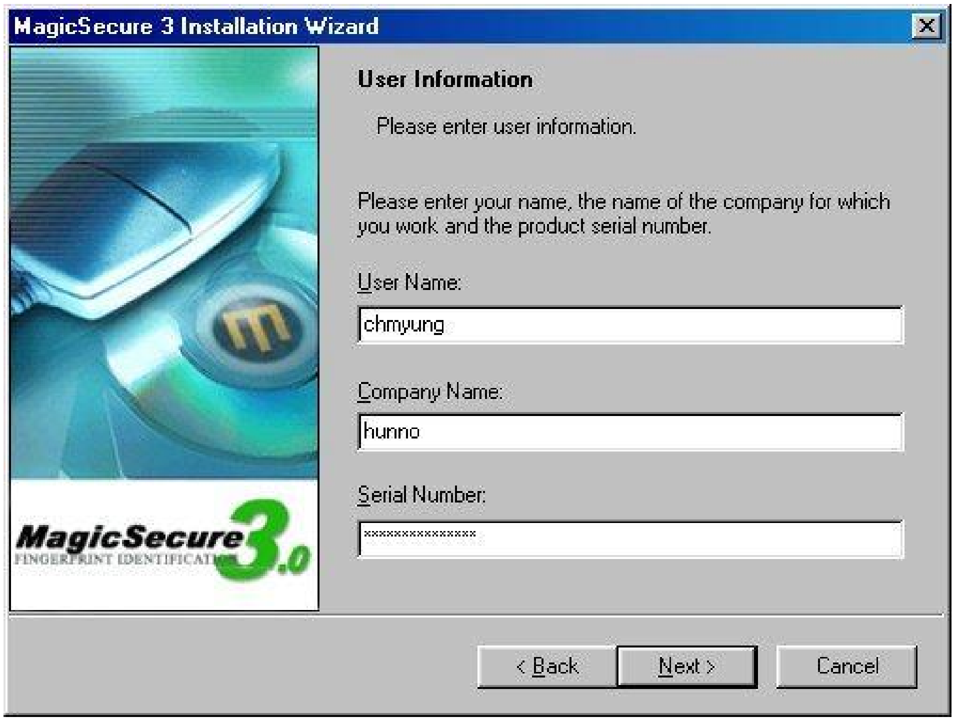
11. Recognition
The user reads and understands the details described in this agreement, agrees with its terms and conditions, and recognizes that its content takes precedence over the old versions of this agreement, order promise, advertisement, notification or other written agreement.

12. Questions
In case there are other questions concerning this agreement, they shall be forwarded to Hunno Technologies Inc. through telephone, fax, e-mail or other means of communication.

You should agree with this agreement to install MagicSecure 3 Standard Edition.

● Agree ○ Disagree

When the **Software License Agreement** window is displayed, read the agreement carefully. If you agree with the terms, select **Agree** and click **Next**.



MagicSecure 3 Installation Wizard

User Information

Please enter user information.

Please enter your name, the name of the company for which you work and the product serial number.

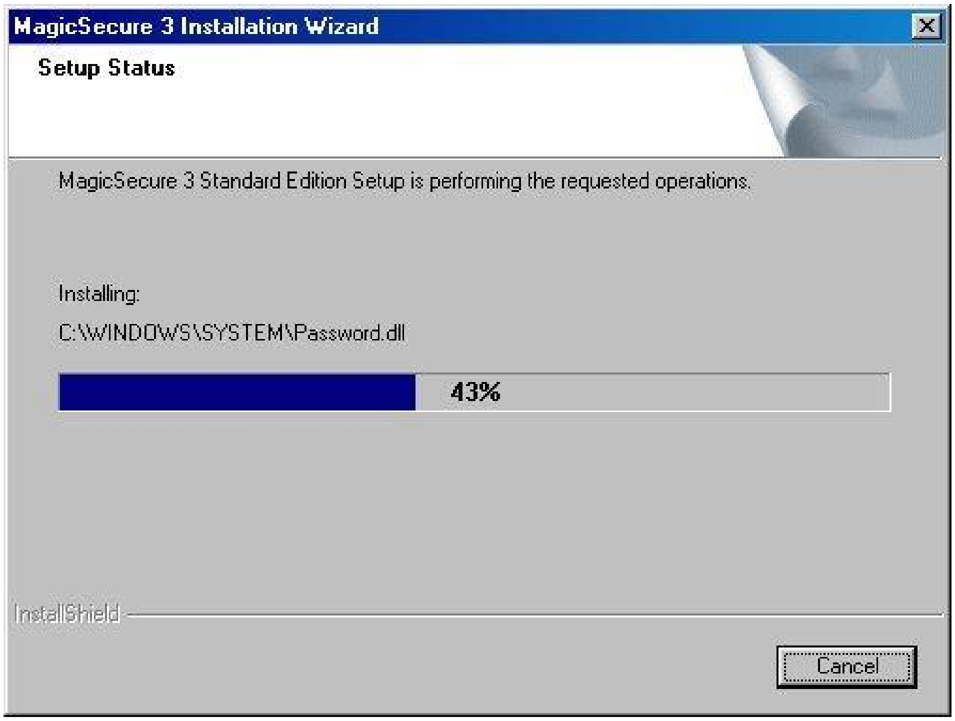
User Name: chmyung

Company Name: hunno

Serial Number: ***************

Input your name, company and the serial number. Click **Next**.

※ Your serial number is indicated in the Software User Certificate provided by Immanuel Electronics Co., Ltd.



MagicSecure 3 Installation Wizard

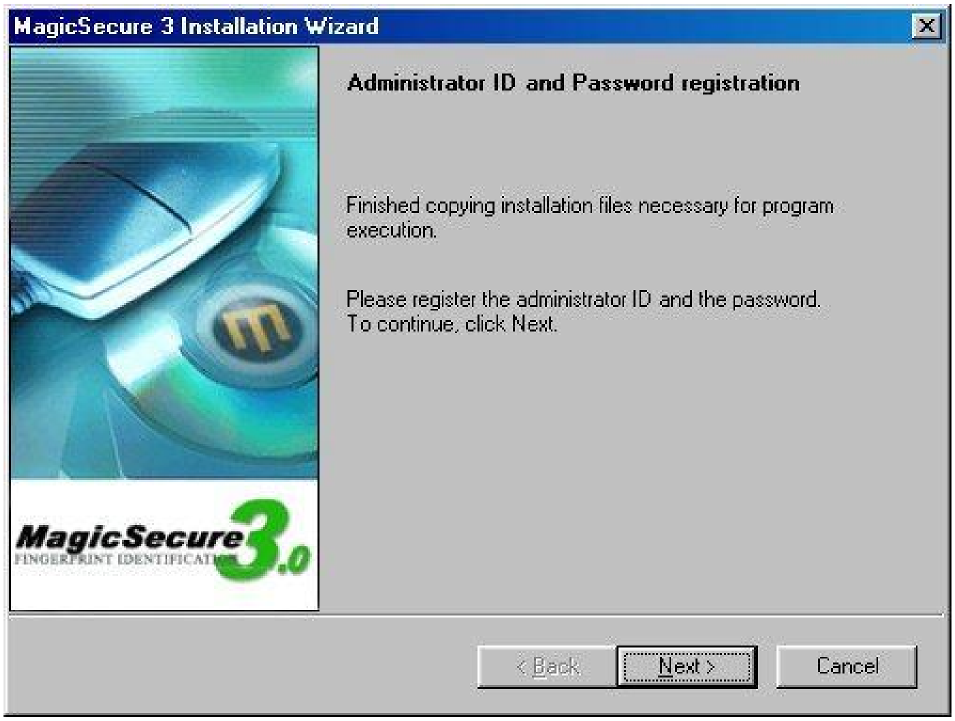
Setup Status

MagicSecure 3 Standard Edition Setup is performing the requested operations.

Installing:
C:\WINDOWS\SYSTEM\Password.dll

43%

Files will be copied to your system for installation.

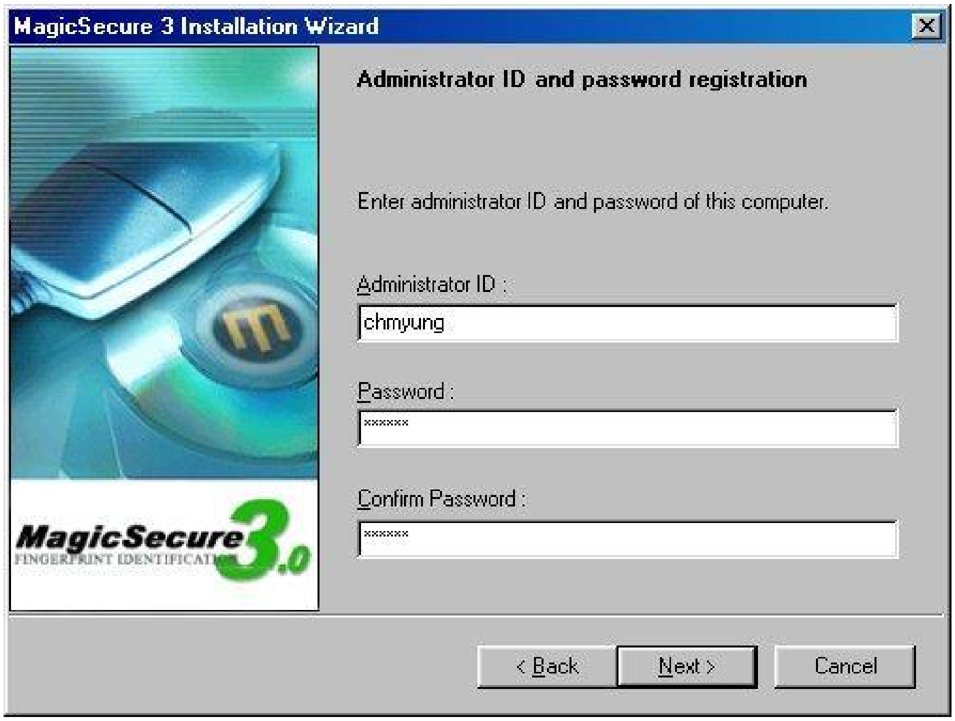


Administrator ID and Password registration

Finished copying installation files necessary for program execution.

Please register the administrator ID and the password.
To continue, click Next.

A message will be displayed indicating that all necessary files are copied to your system. Click **Next**.



Administrator ID and password registration

Enter administrator ID and password of this computer.

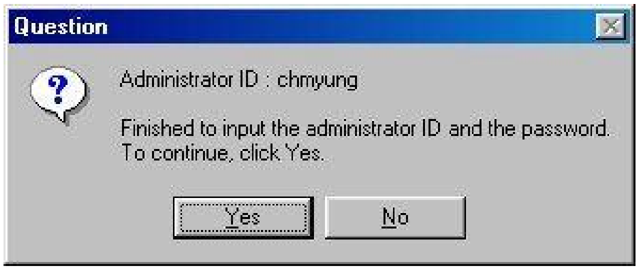
Administrator ID : chmyung

Password : ******

Confirm Password : ******

Input the **Administrator ID** and **Password**. Confirm your password in the **Confirm Password** window.

Verify whether the information you provided is correct. If so, click **Next**.



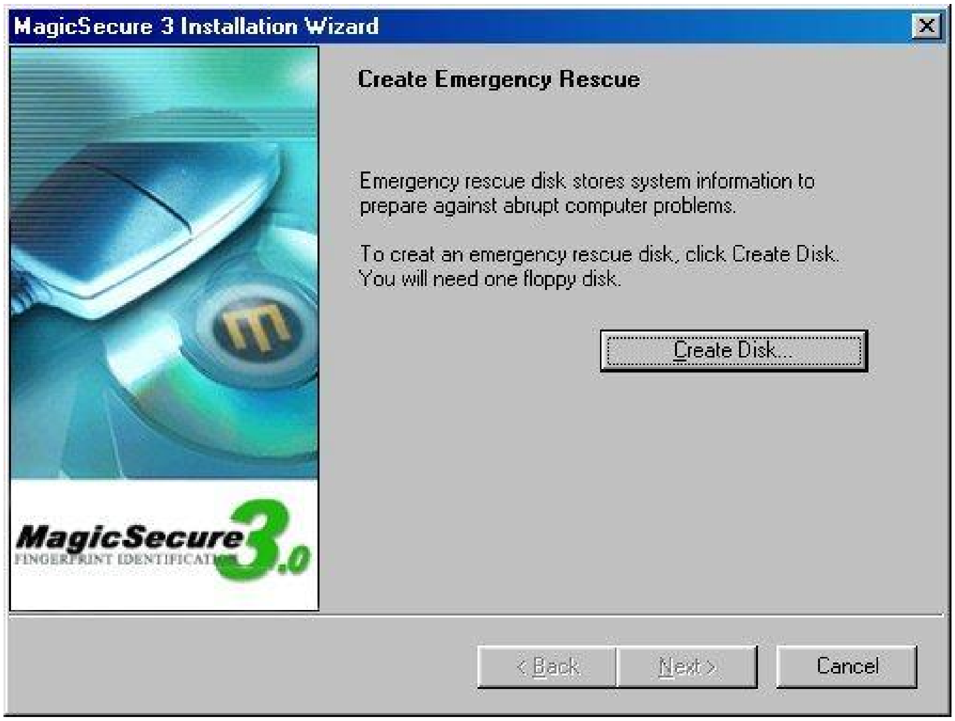
Administrator ID : chmyung

Finished to input the administrator ID and the password.
To continue, click Yes.

A message box will be displayed confirming the **Administrator ID** you provided.

If the ID you provided is correct, click **Yes**.

*** If you do not wish to create an Emergency Rescue Disk**



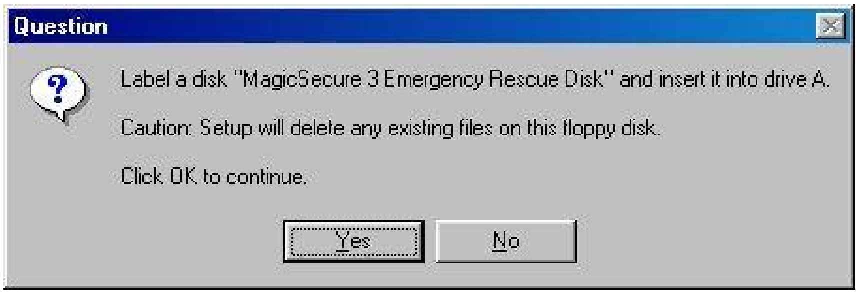
MagicSecure 3 Installation Wizard

Create Emergency Rescue

Emergency rescue disk stores system information to prepare against abrupt computer problems.

To creat an emergency rescue disk, click Create Disk. You will need one floppy disk.

Click **Create Disk…**.



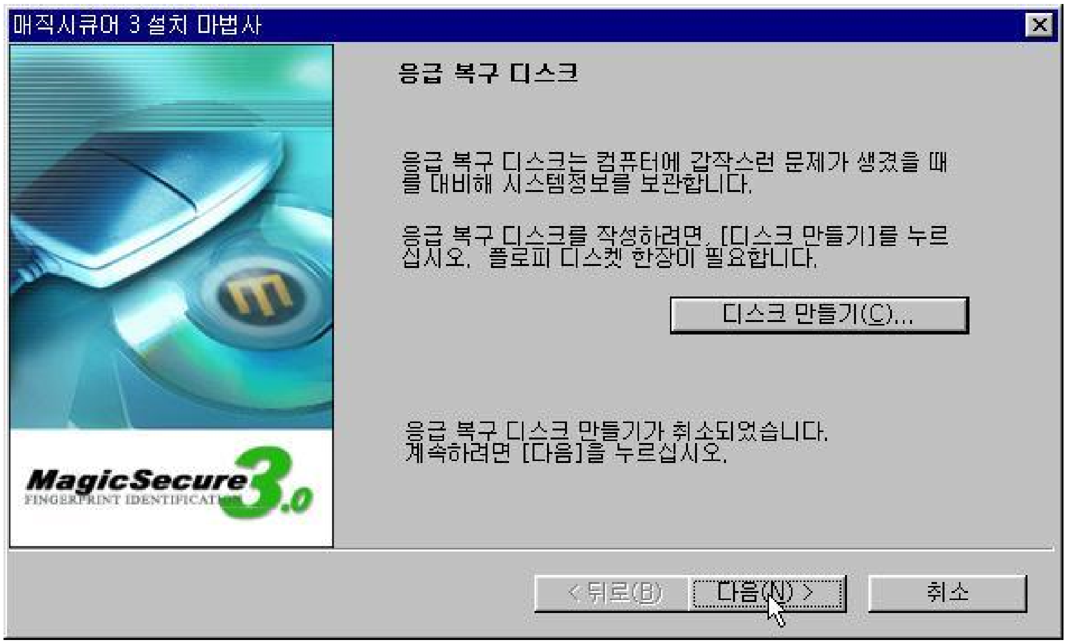
Question

Label a disk "MagicSecure 3 Emergency Rescue Disk" and insert it into drive A.

Caution: Setup will delete any existing files on this floppy disk.

Click OK to continue.

Without inserting a floppy disk into drive A: and click **No**.



응급 복구 디스크

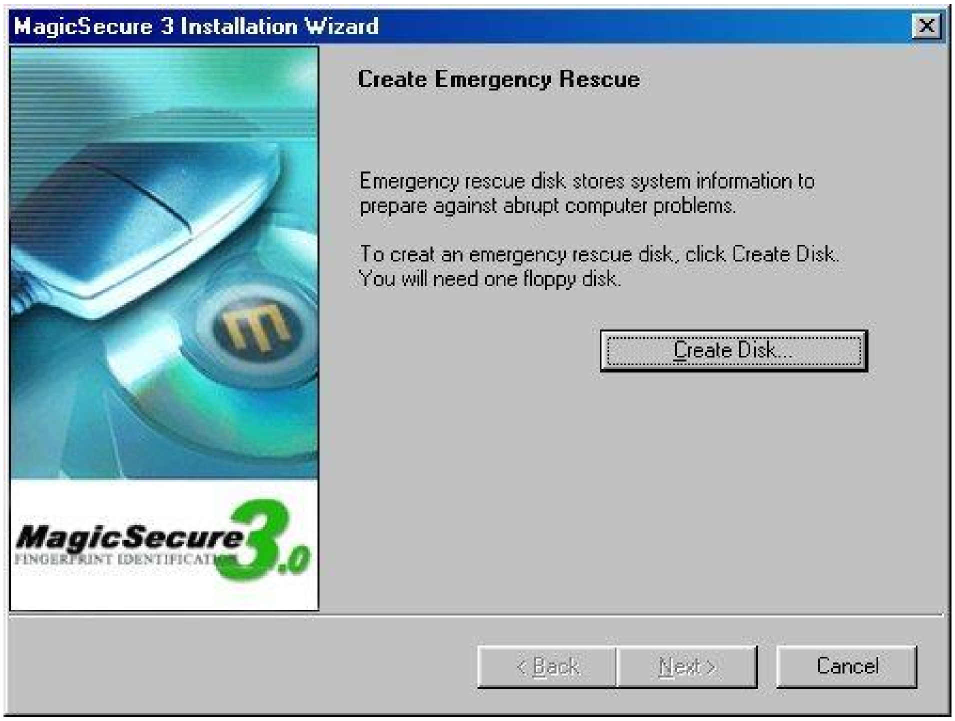
응급 복구 디스크는 컴퓨터에 갑작스런 문제가 생겼을 때를 대비해 시스템정보를 보관합니다.

응급 복구 디스크를 작성하려면, [디스크 만들기]를 누르십시오. 플로피 디스켓 한장이 필요합니다.

응급 복구 디스크 만들기가 취소되었습니다.
계속하려면 [다음]을 누르십시오.

Acknowledging that you do not wish to create an Emergency Rescue Disk, the **Next** button will be activated, click **Next**.

*** If you wish to create an Emergency Rescue Disk (Required)**



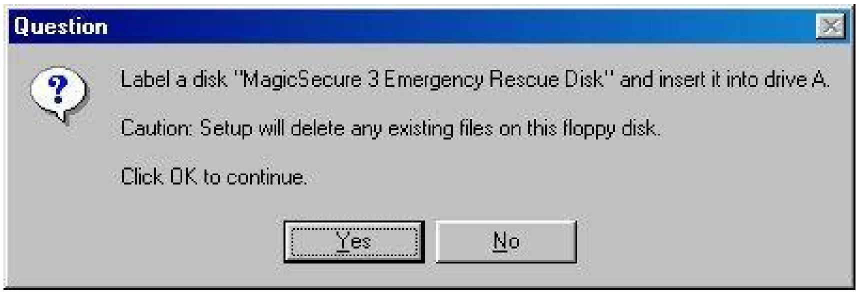
MagicSecure 3 Installation Wizard

Create Emergency Rescue

Emergency rescue disk stores system information to prepare against abrupt computer problems.

To creat an emergency rescue disk, click Create Disk. You will need one floppy disk.

Click **Create Disk…**.



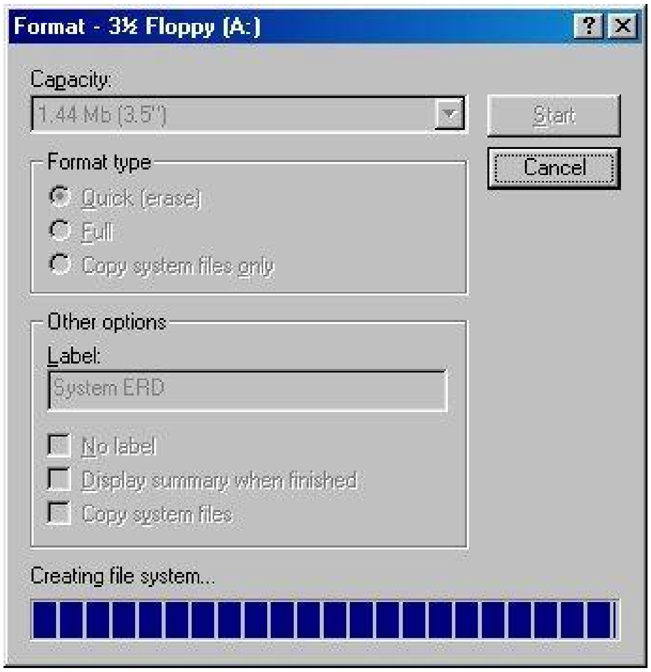
Question

Label a disk "MagicSecure 3 Emergency Rescue Disk" and insert it into drive A.

Caution: Setup will delete any existing files on this floppy disk.

Click OK to continue.

Insert a blank floppy disk into drive A: and click **Yes**.



Format - 3½ Floppy (A:)

Capacity: 1.44 Mb (3.5")

Format type

- ● Quick (erase)
- ○ Full
- ○ Copy system files only

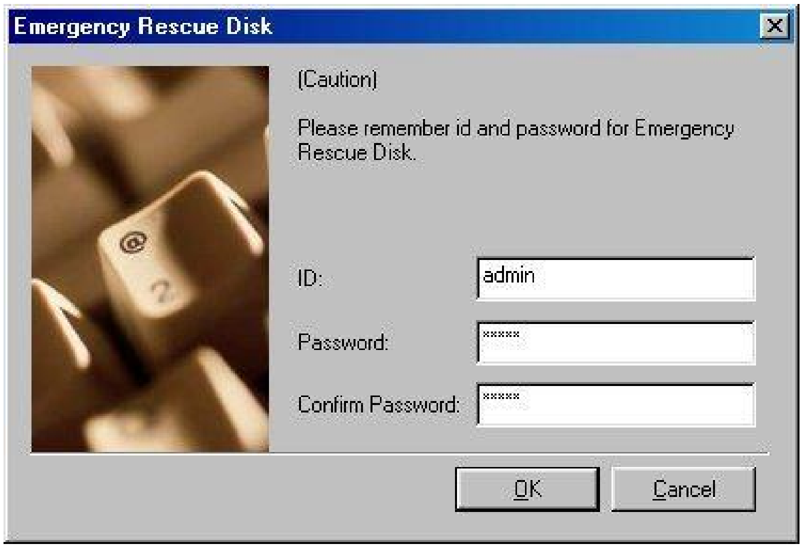
Other options

Label: System ERD

- □ No label
- □ Display summary when finished
- □ Copy system files

Creating file system...

Ramses II will create an **Emergency Rescue Disk** in drive A:



Emergency Rescue Disk

(Caution)

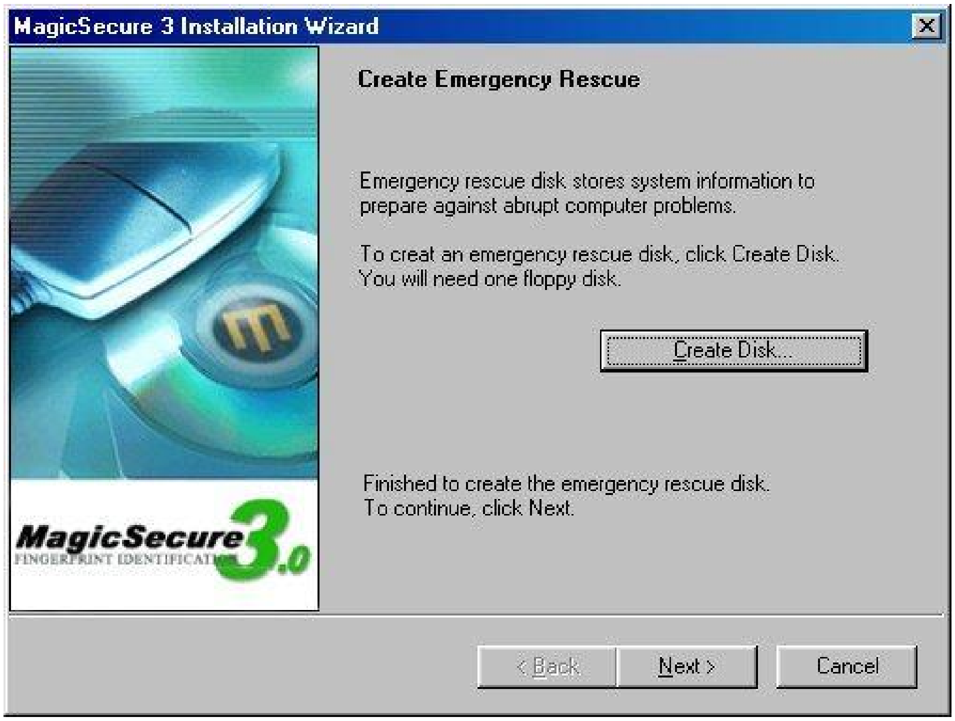
Please remember id and password for Emergency Rescue Disk.

ID: admin

Password: *****

Confirm Password: *****

Input an ID and password for the **Emergency Rescue Disk**. (You can provide a random ID and password at your discretion)



MagicSecure 3 Installation Wizard

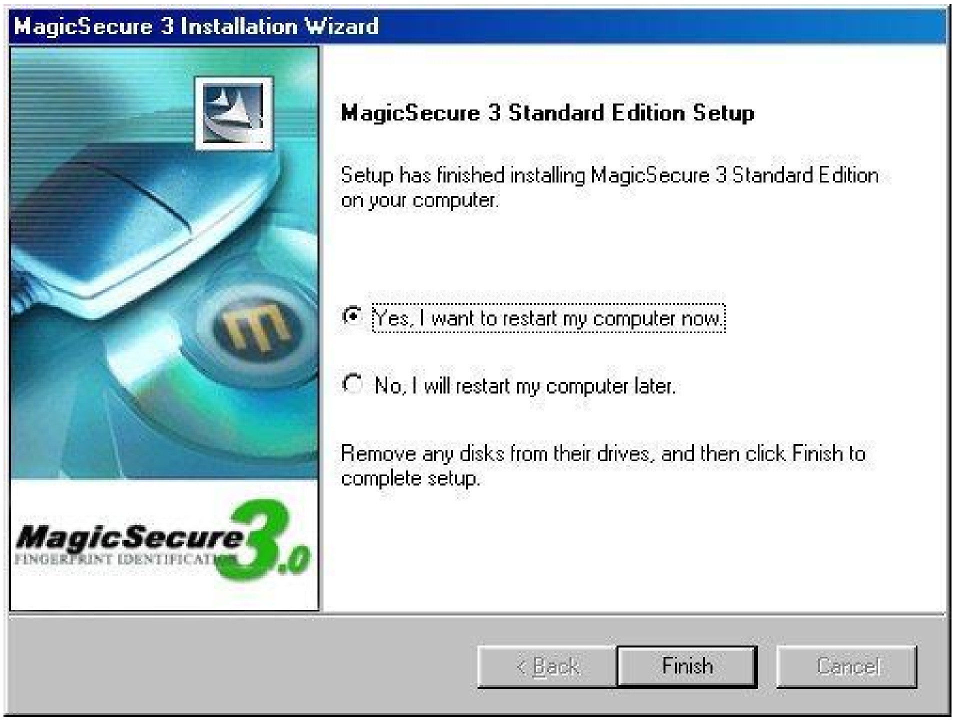
Create Emergency Rescue

Emergency rescue disk stores system information to prepare against abrupt computer problems.

To creat an emergency rescue disk, click Create Disk. You will need one floppy disk.

Finished to create the emergency rescue disk. To continue, click Next.

After the **Emergency Rescue Disk** has been created, click **Next**.



MagicSecure 3 Installation Wizard

MagicSecure 3 Standard Edition Setup

Setup has finished installing MagicSecure 3 Standard Edition on your computer.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

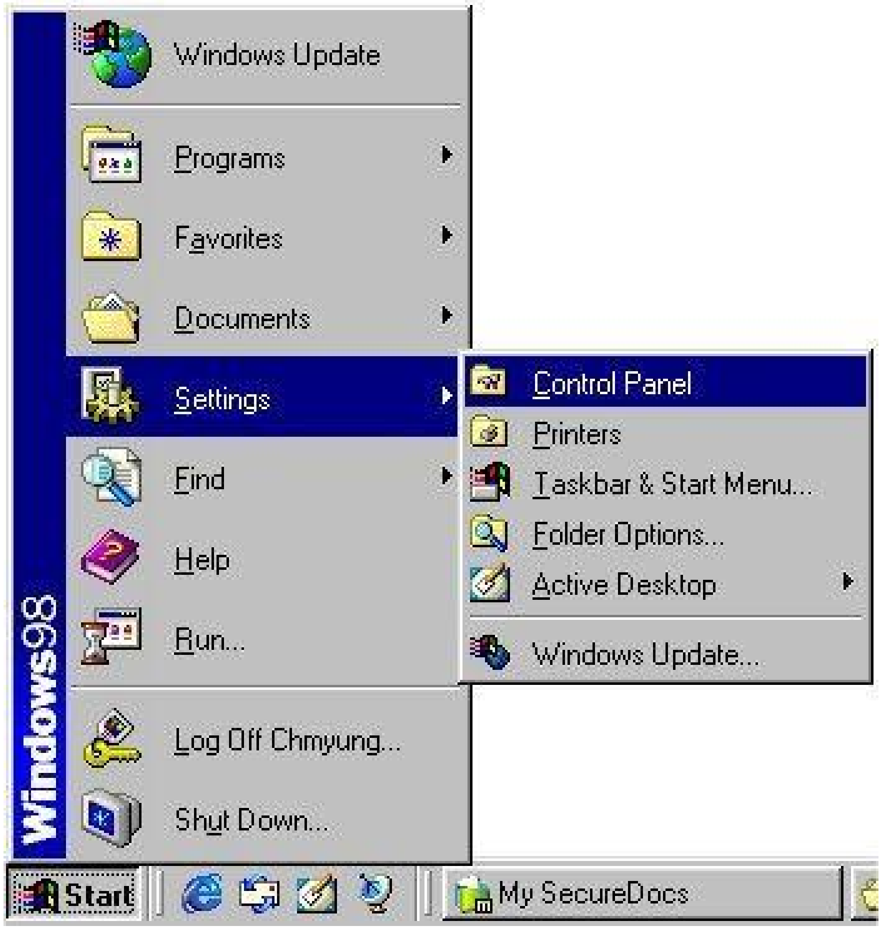
A message will be displayed indicating that Ramses II has been installed on your system. Click **Finish** to complete the installation procedure. Ramses II will reboot your system.

Ramses II is now successfully installed on your system.

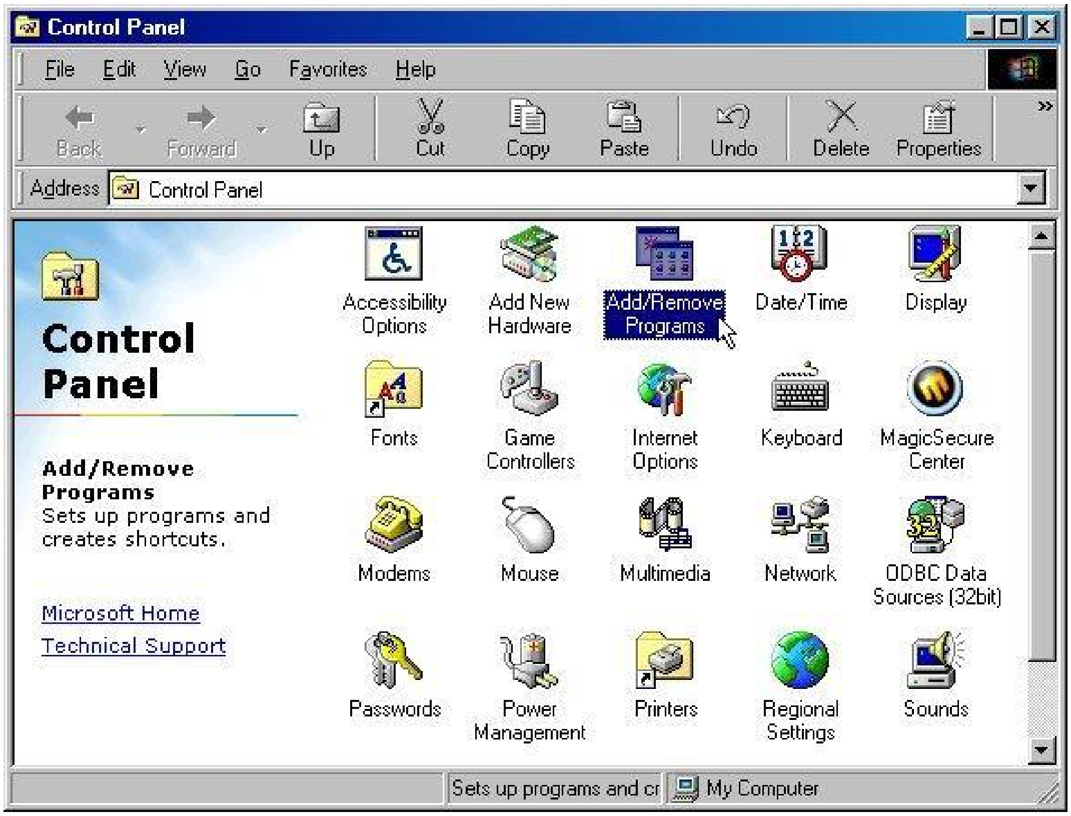
Chapter 2. Uninstall Program

Only users with administrator authorities can remove Ramses II from the system.

Administrator authorities can be granted when a new user is registered from the **Ramses II Center**.

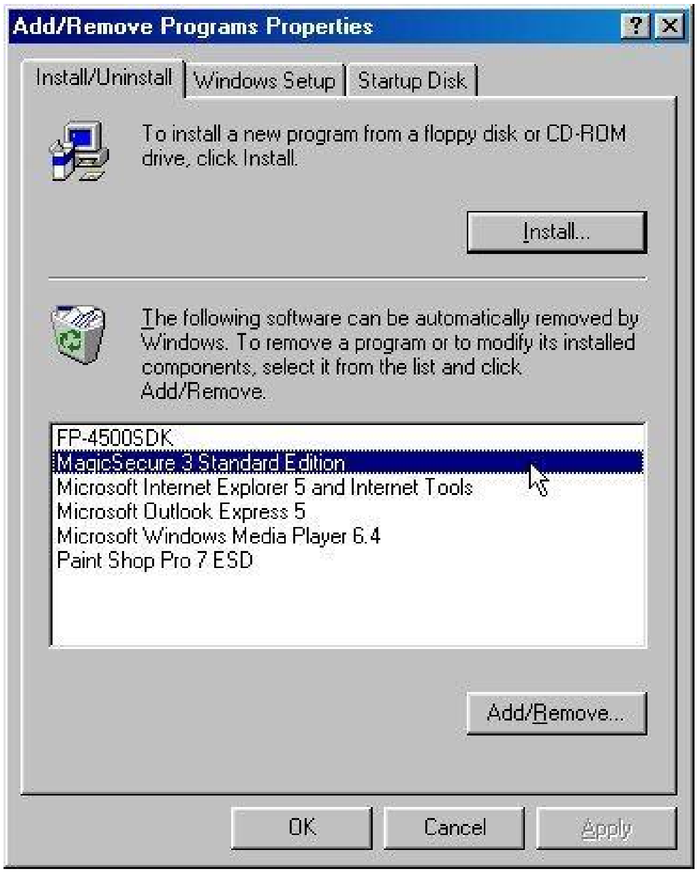


From the taskbar, select **Start > Settings > Control Panel**.



Add/Remove Programs
Sets up programs and creates shortcuts.

From the **Control Panel** window, double-click **Add/Remove Programs**.

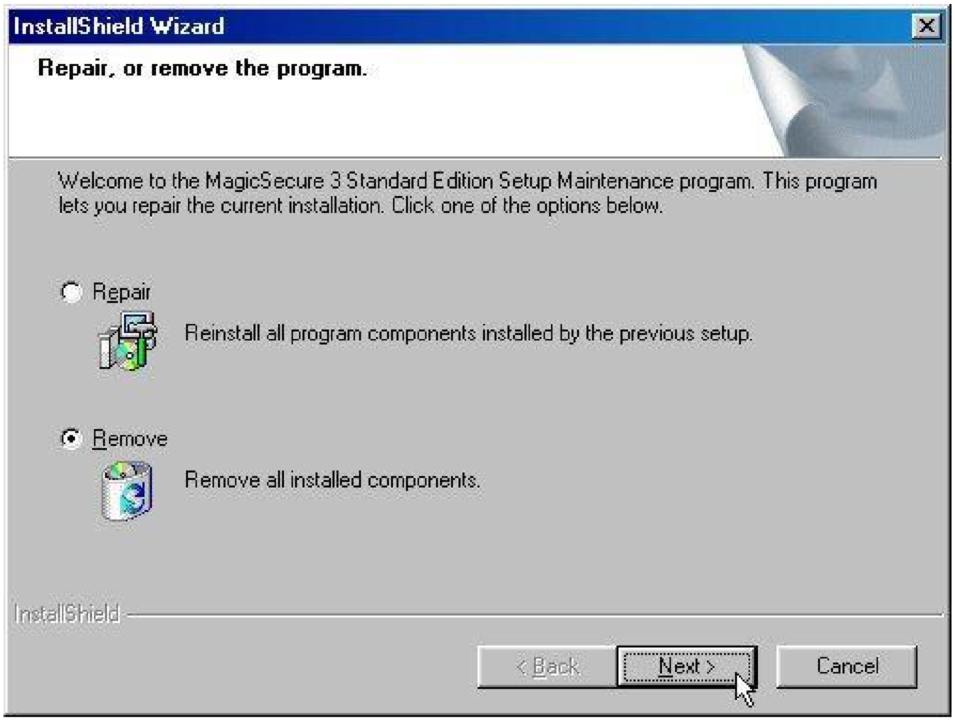


To install a new program from a floppy disk or CD-ROM drive, click Install.

The following software can be automatically removed by Windows. To remove a program or to modify its installed components, select it from the list and click Add/Remove.

FP-4500SDK
MagicSecure 3 Standard Edition
Microsoft Internet Explorer 5 and Internet Tools
Microsoft Outlook Express 5
Microsoft Windows Media Player 6.4
Paint Shop Pro 7 ESD

Select the **Install/Uninstall** tab, choose **Ramses II Standard Edition**, and click **Add/Remove…**.



InstallShield Wizard

Repair, or remove the program.

Welcome to the MagicSecure 3 Standard Edition Setup Maintenance program. This program lets you repair the current installation. Click one of the options below.

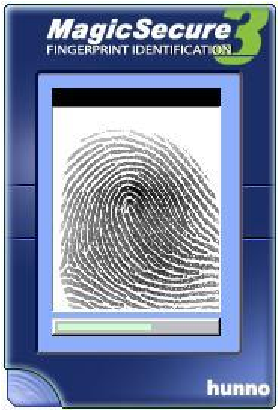
○ Repair

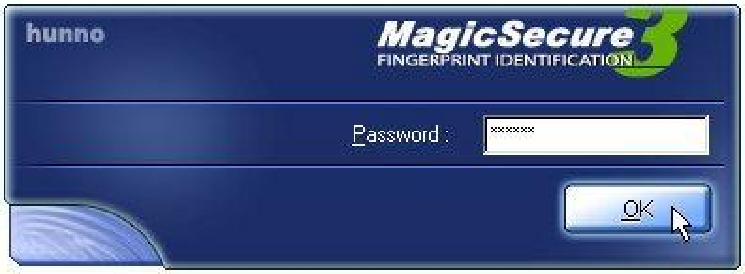
Reinstall all program components installed by the previous setup.

● Remove

Remove all installed components.

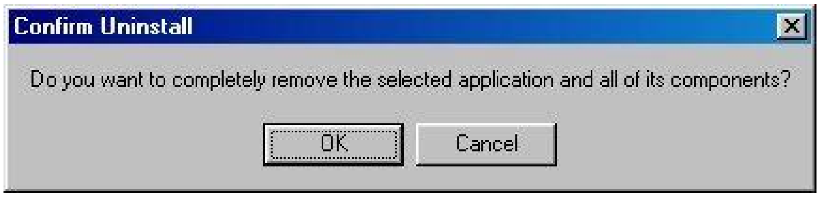
Select **Remove** and click **Next**.





Password : ******

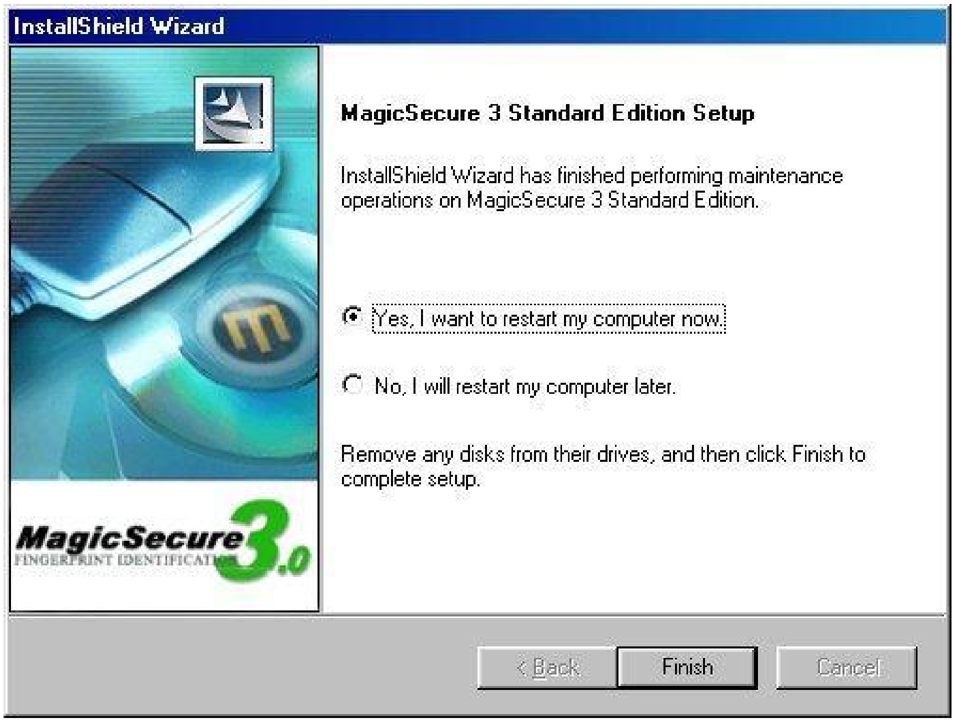
Provide the administrator's fingerprint or password and click **OK**.



Confirm Uninstall

Do you want to completely remove the selected application and all of its components?

A message box will be displayed asking you whether you wish to remove the program. Click **OK**.



InstallShield Wizard

MagicSecure 3 Standard Edition Setup

InstallShield Wizard has finished performing maintenance operations on MagicSecure 3 Standard Edition.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

After Ramses II is successfully removed, click **Finish** to reboot your system.

Chapter 3. Introduction to Features

1. Ramses II Center

Ramses II Center is responsible for Ramses II ver3.0's key features including user dministration(registration/modification/deletion), authorities, system configuration and **log maintenance**.

ⓐ User/Group Administration

- An administrator can grant authorities to each computer user.
- A user can be registered/modified/deleted, and the corresponding user information can be stored from the Ramses II Center.
- Maintaining users in groups facilitates the administration work.
- Ramses II Center allows each user to register/modify/delete fingerprints, change passwords and select the identification method.

ⓑ System Configuration

- System configuration can be modified by an administrator or a super user.
- Selects the log-on ID display (text box/combo box)
- Controls the identification method for standard users
- Sets whether the F5 or F8 key will be used for booting the system for protection purposes
- Selects the encryption algorithm, and whether a fingerprint recognition mouse or device will be used

ⓒ Log Maintenance

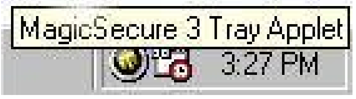
- Ramses II Center records a log fie regarding log-on, encryption and system configuration.
- You can view or print a specified date's log file.

ⓓ Emergency Rescue Disk

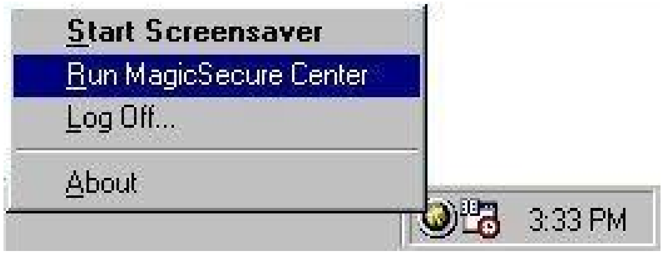
- You can reset your system configuration to the point when the Emergency Rescue Disk was created.
- You can create an Emergency Rescue Disk for errors that occurred during a Ramses II operation.

(1) How to Run Ramses II Center

① Method 1: Running from the Tray Icon



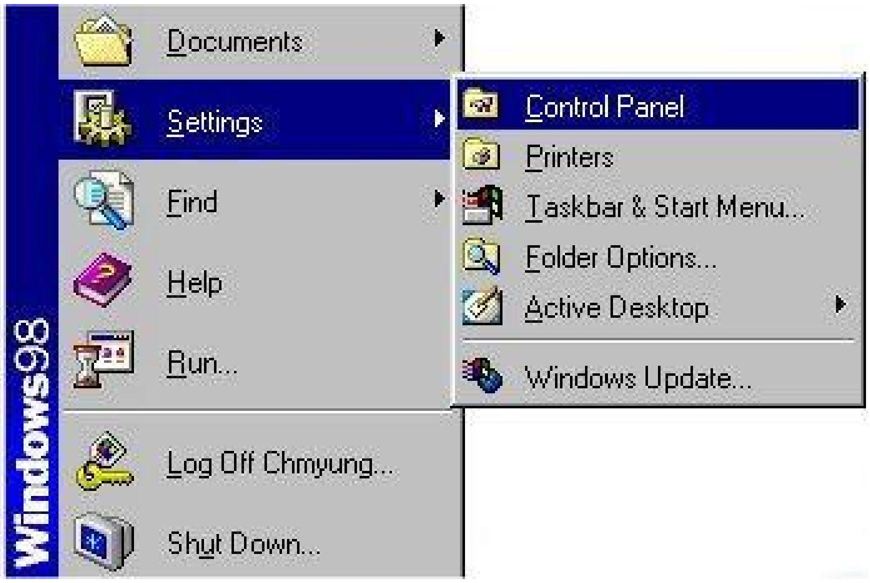
Right-click the **Ramses Tray Applet** icon on the Tray Bar.



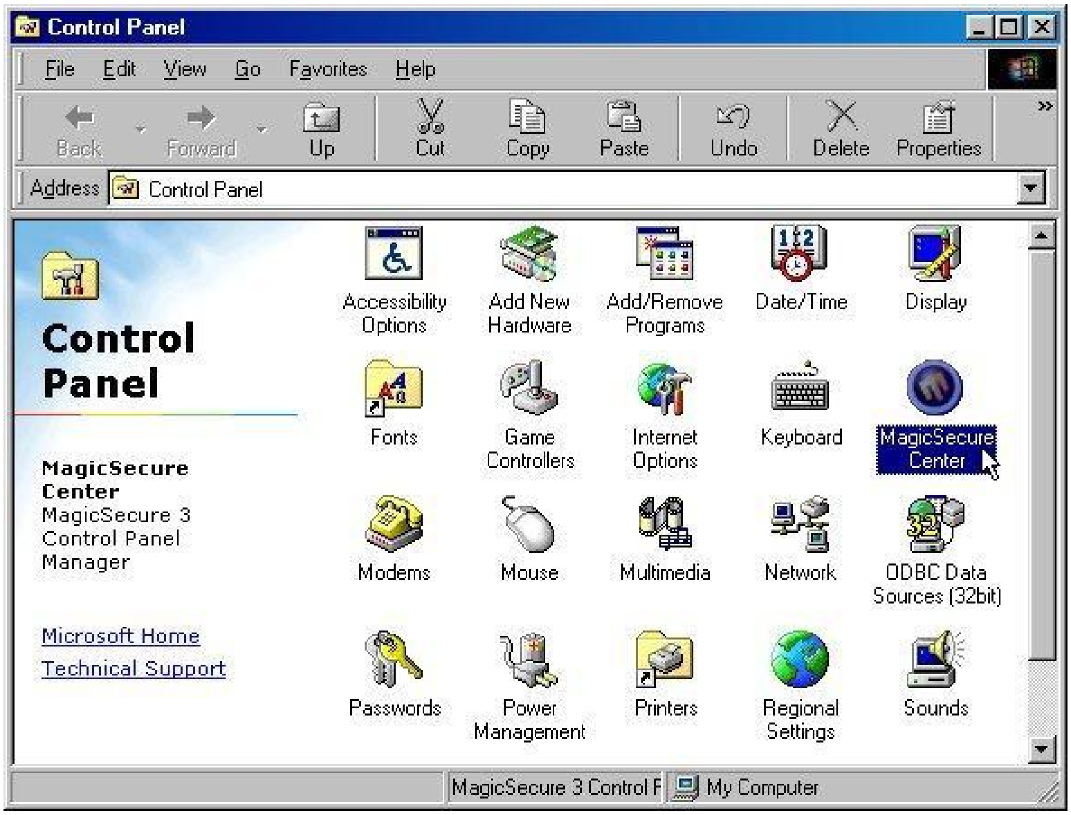
Select **Run Ramses II Center**.

② Method 2: Start > Settings > Control Panel > Run Ramses II Center

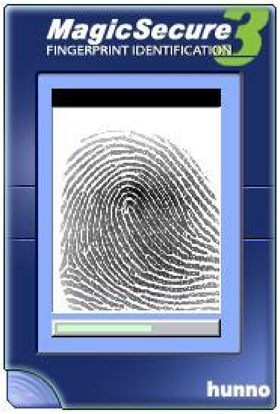
Select **Start > Settings > Control Panel**.

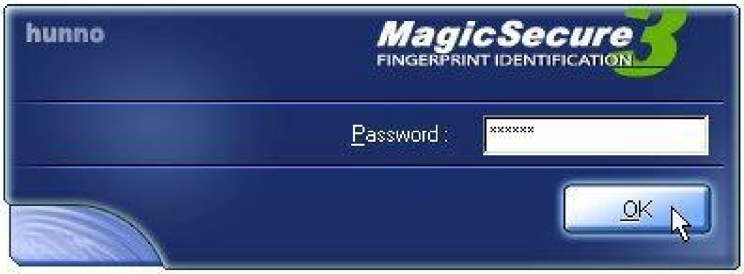


From the taskbar, select **Start > Settings > Control Panel**.



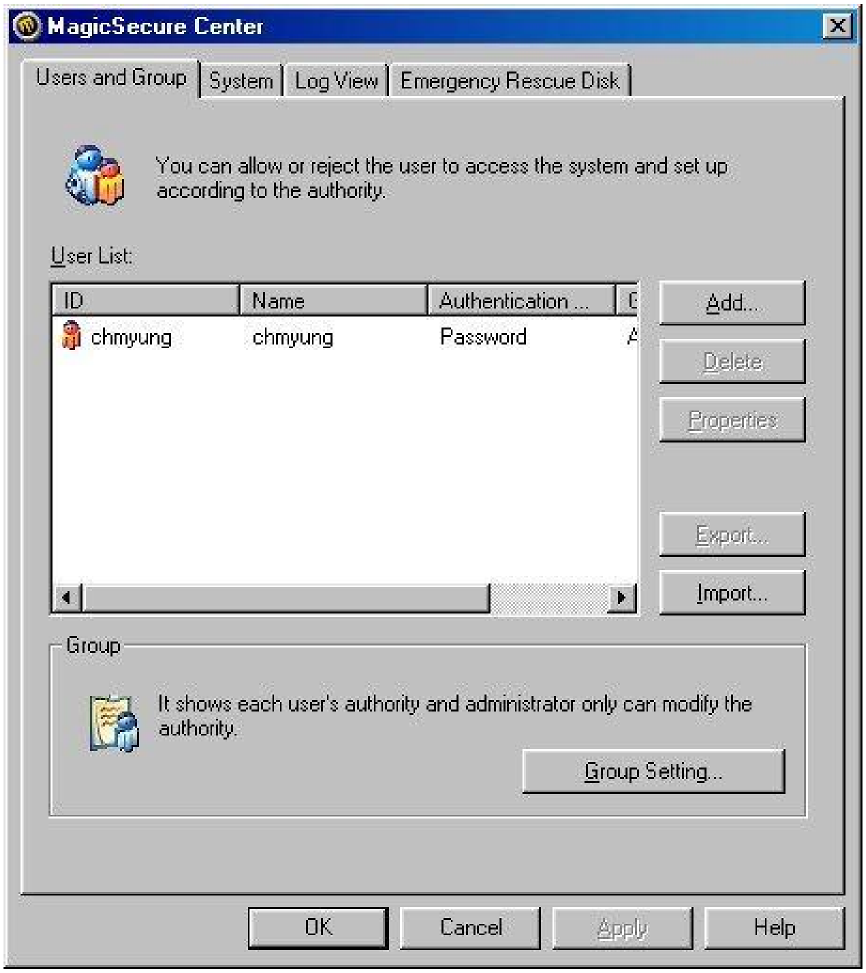
From the **Control Panel** window, double-click the **Rmses II Center** icon.





Provide a registered user's fingerprint or password.

Those not registered in the **Users and Group** cannot use the **Ramses II Center**.



You can allow or reject the user to access the system and set up according to the authority.

ID	Name	Authentication ...
chmyung	chmyung	Password

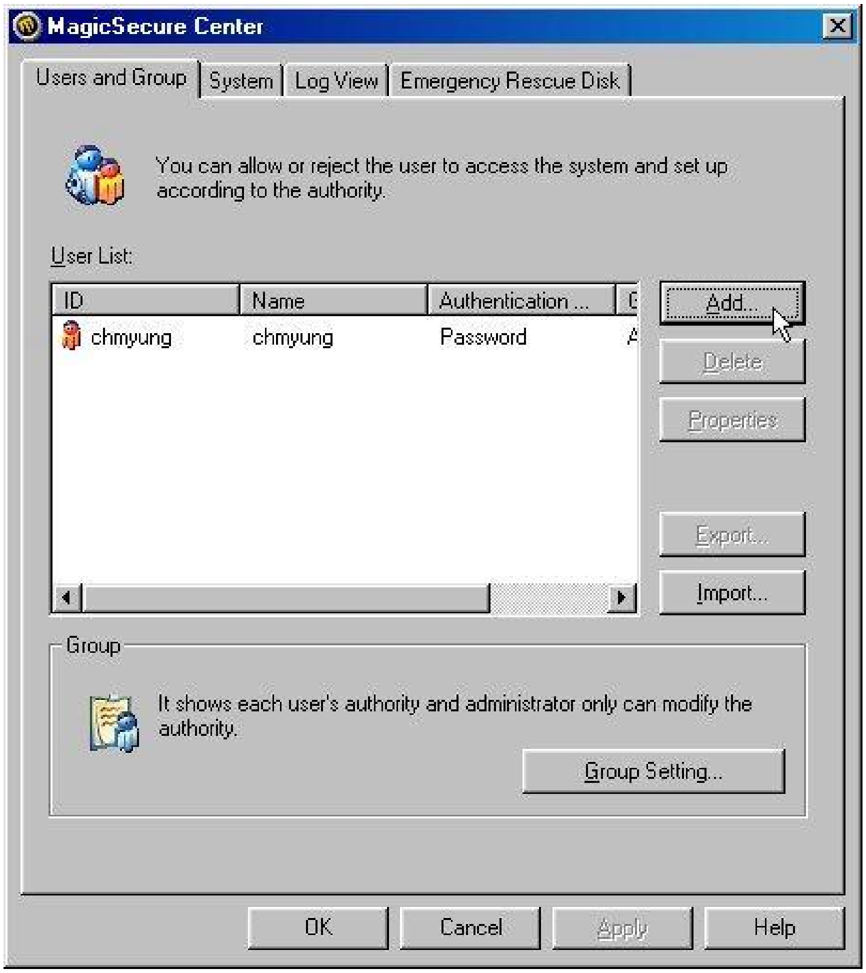
It shows each user's authority and administrator only can modify the authority.

The figure above displays the **Ramses II Center** running.

(2) User and Group Management

- An administrator can add/delete users and modify user information.
- Standard users can only modify their own information.

① Add a user



You can allow or reject the user to access the system and set up according to the authority.

User List:

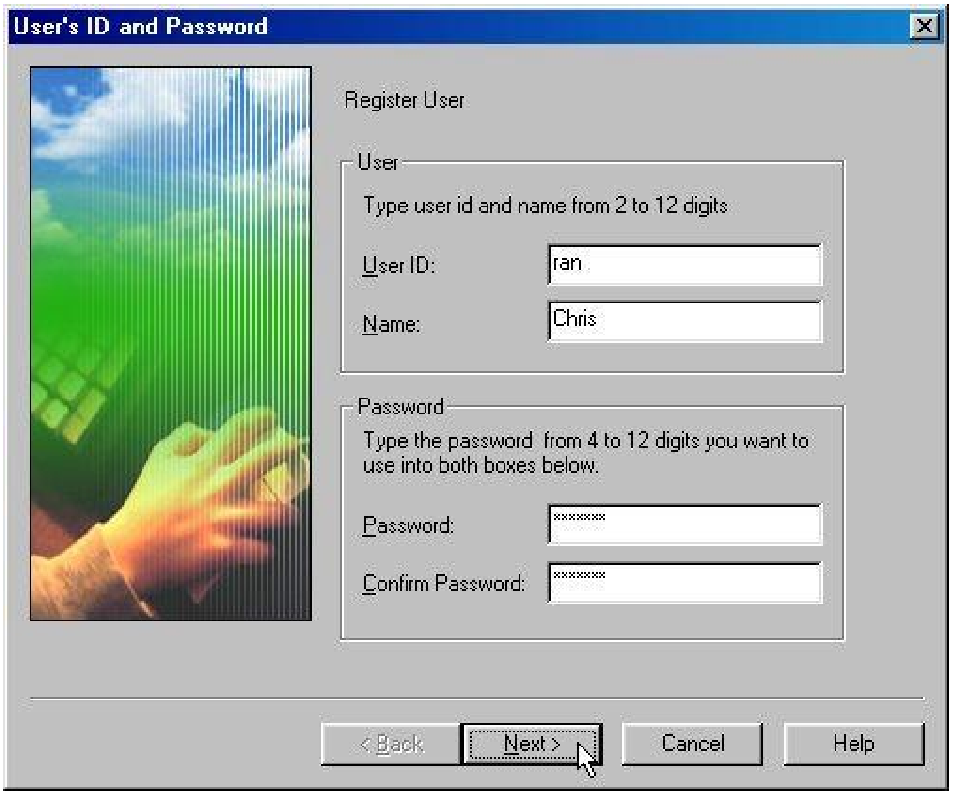
ID	Name	Authentication ...	G
chmyung	chmyung	Password	A

Group

It shows each user's authority and administrator only can modify the authority.

Select the **Users and Group** tab and click **Add**.

Registering new user ID and password



Register User

User

Type user id and name from 2 to 12 digits

User ID: ran

Name: Chris

Password

Type the password from 4 to 12 digits you want to use into both boxes below.

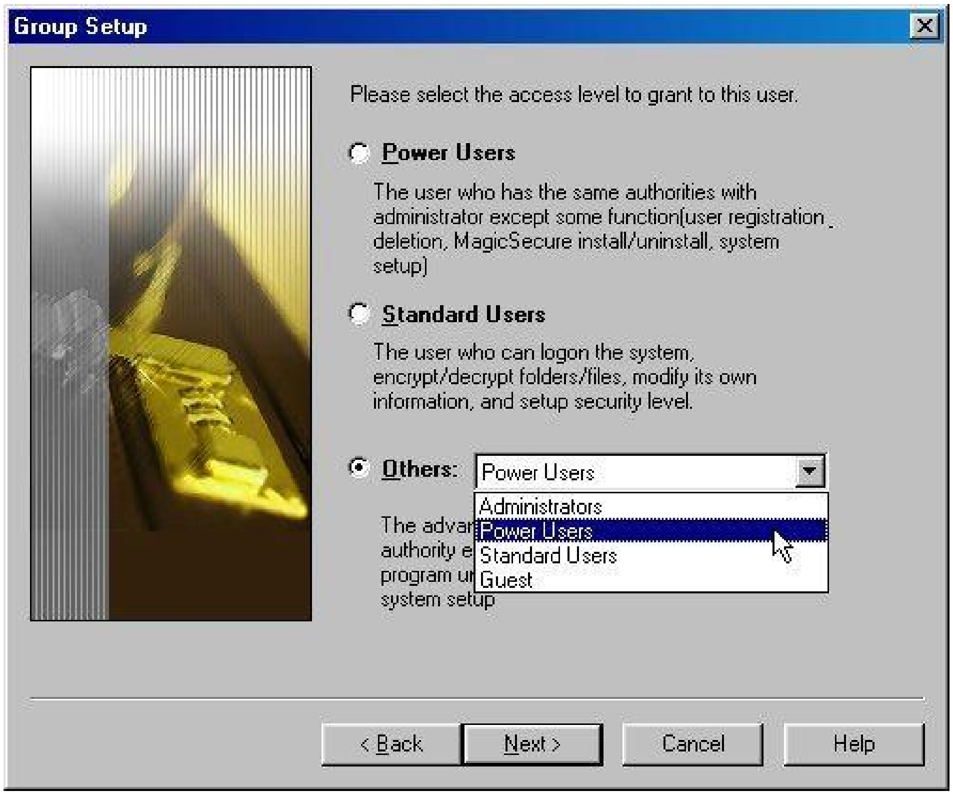
Password: xxxxxxx

Confirm Password: xxxxxxx

Provide the user information and click **Next**. (Password must consist of four or more characters)

Group Authorities

- Administrators: Has every access right to the computer and can manage every user.
- Power Users: Has similar rights as an administrator but a few functions such as user registration, Ramses II removal and system configuration.
- Standard Users: Can log on to the system, encrypt/decrypt folders/files, modify one's own information and set security levels.
- Guest: Can only log on to the system, and cannot encrypt/decrypt files or even modify one's own information.



Group Setup

Please select the access level to grant to this user.

○ Power Users

The user who has the same authorities with administrator except some function(user registration , deletion, MagicSecure install/uninstall, system setup)

○ Standard Users

The user who can logon the system, encrypt/decrypt folders/files, modify its own information, and setup security level.

● Others: Power Users

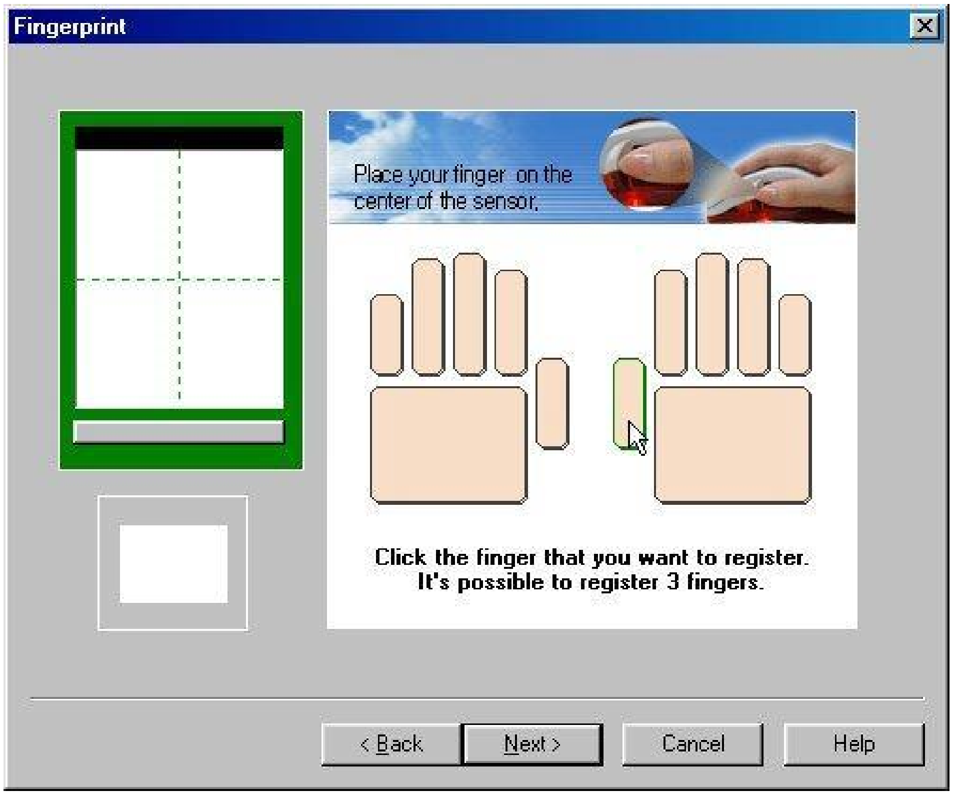
The advar authority e program ur system setup

Select the user's access level and click **Next**.

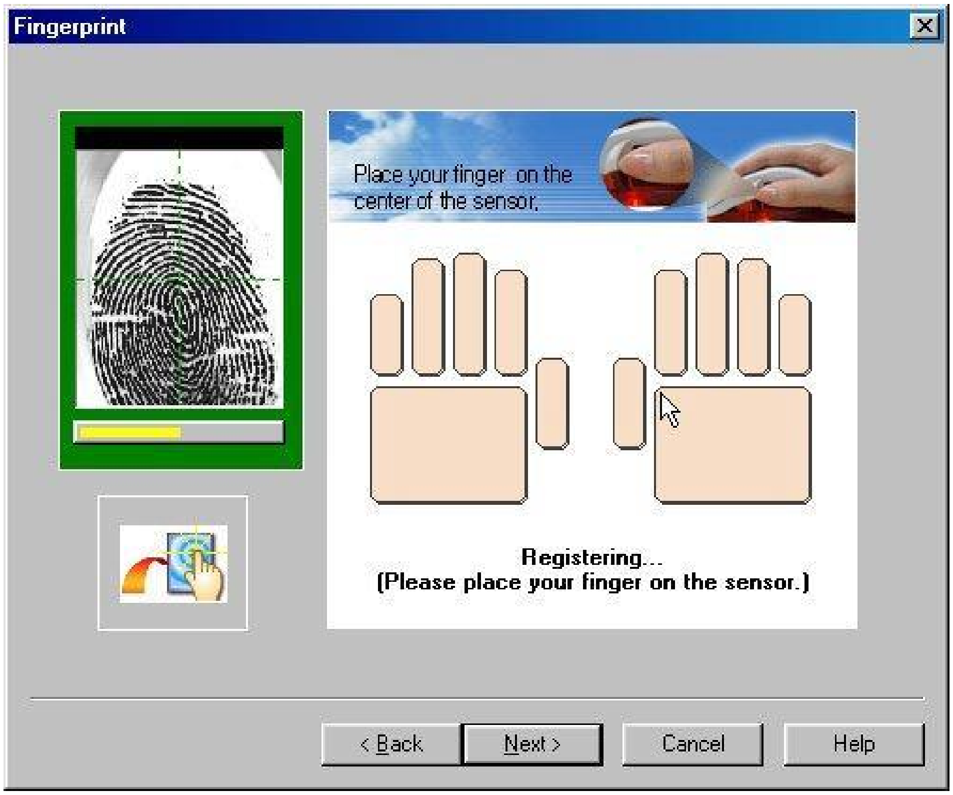
How to register a fingerprint

A user must register one or more fingerprints. (Up to three fingerprints can be registered)

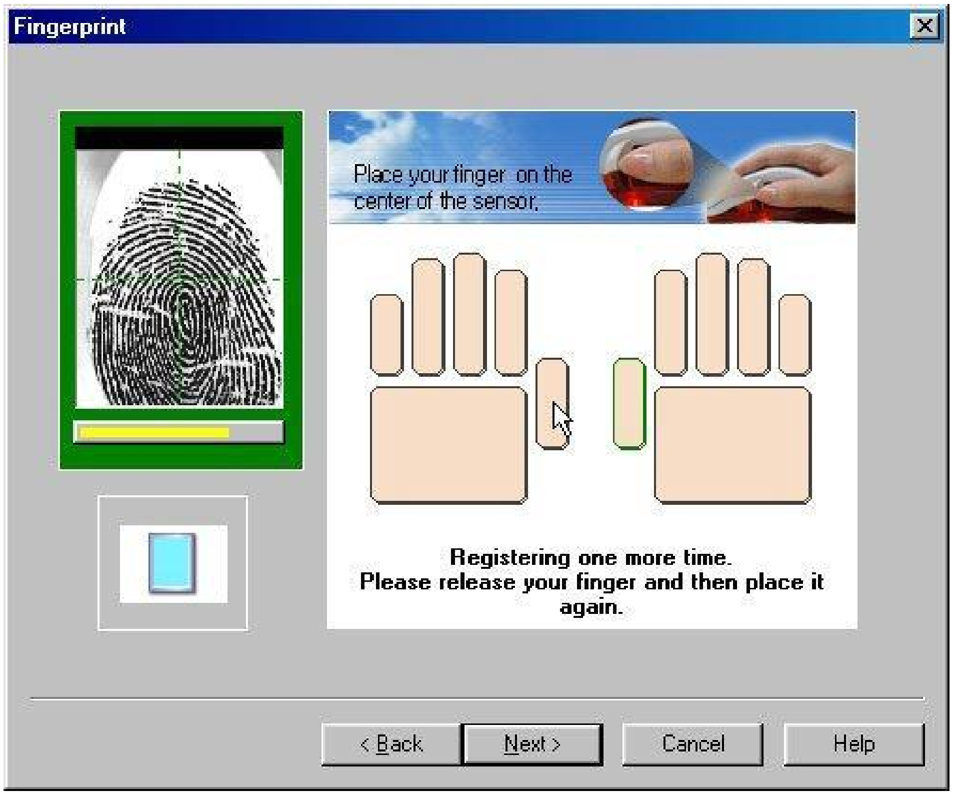
- Select a finger that you wish to register the print of.
- A message will be displayed indicating that the information is being registered.
- Place the selected finger on the fingerprint sensor.
- A message will be displayed asking you to remove your finger and place it back on the sensor.
- Remove your finger -> The **Registering…** message will be displayed.
- Place the selected finger on the fingerprint sensor again.
- Register prints of other fingers by following these steps.



Click the finger that you want to register.
It's possible to register 3 fingers.



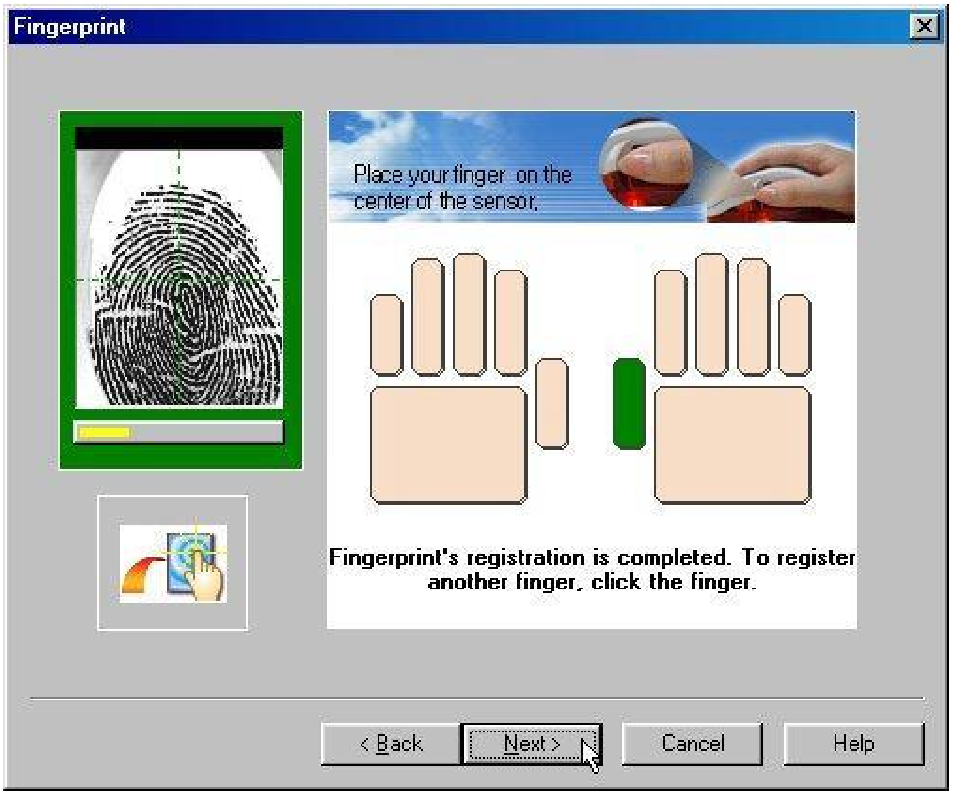
Registering...
(Please place your finger on the sensor.)



Fingerprint

Place your finger on the center of the sensor.

Registering one more time.
Please release your finger and then place it again.



Fingerprint

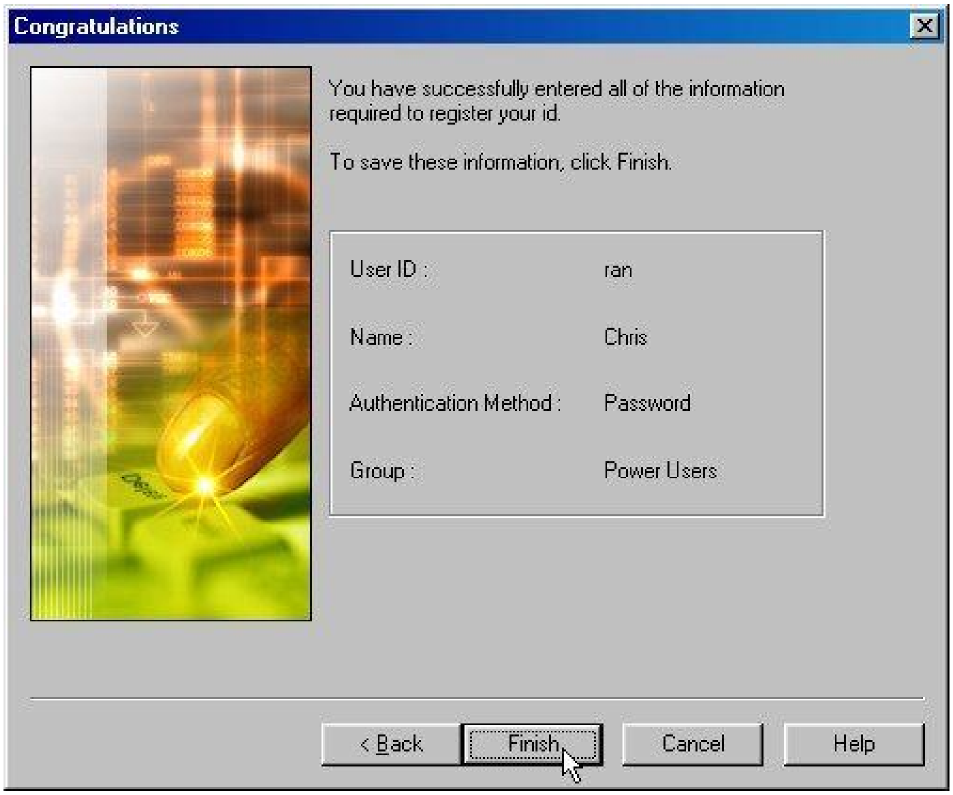
Place your finger on the center of the sensor.

Fingerprint's registration is completed. To register another finger, click the finger.

This is the final step of the user registration procedure.

The registered user information will be displayed for verification.

Finish



You have successfully entered all of the information required to register your id.

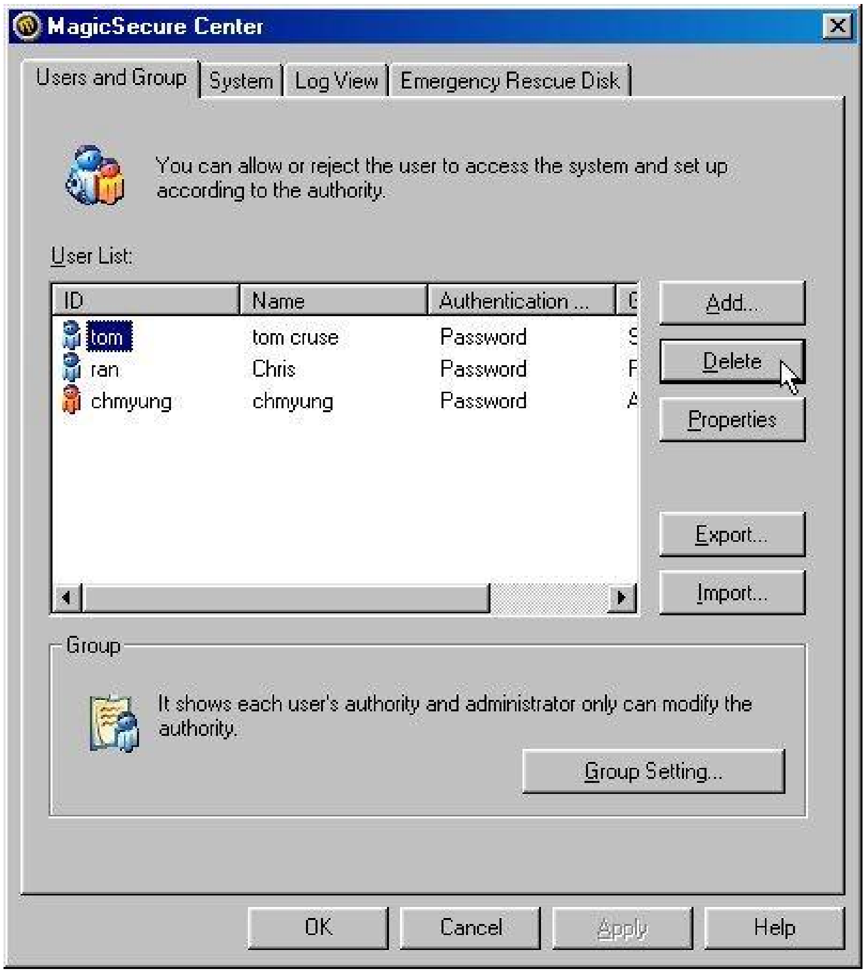
To save these information, click Finish.

User ID :	ran
Name :	Chris
Authentication Method :	Password
Group :	Power Users

If the displayed information is correct, click **Finish**.

② **Delete a user**

- Only an administrator can delete a user.
- A deleted user cannot be recovered.



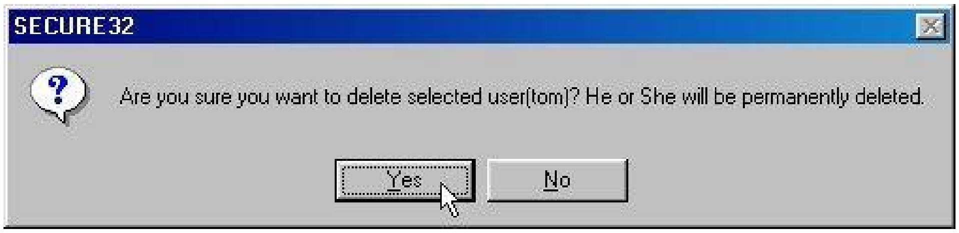
You can allow or reject the user to access the system and set up according to the authority.

User List:

ID	Name	Authentication ...	G
tom	tom cruse	Password	S
ran	Chris	Password	F
chmyung	chmyung	Password	A

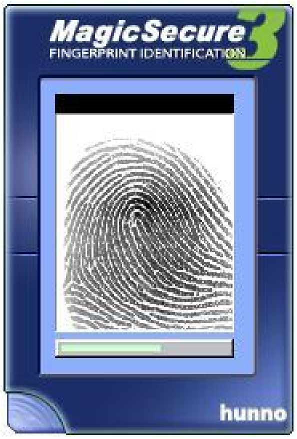
It shows each user's authority and administrator only can modify the authority.

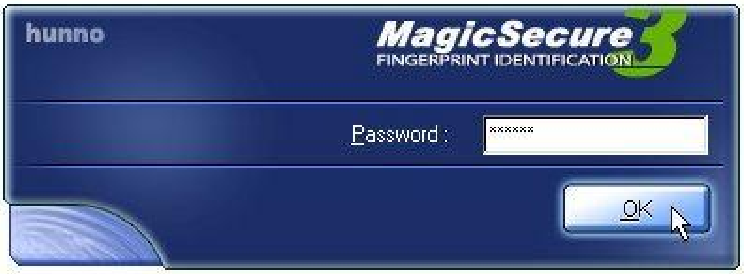
Select the user you wish to delete and click **Delete**.



Are you sure you want to delete selected user(tom)? He or She will be permanently deleted.

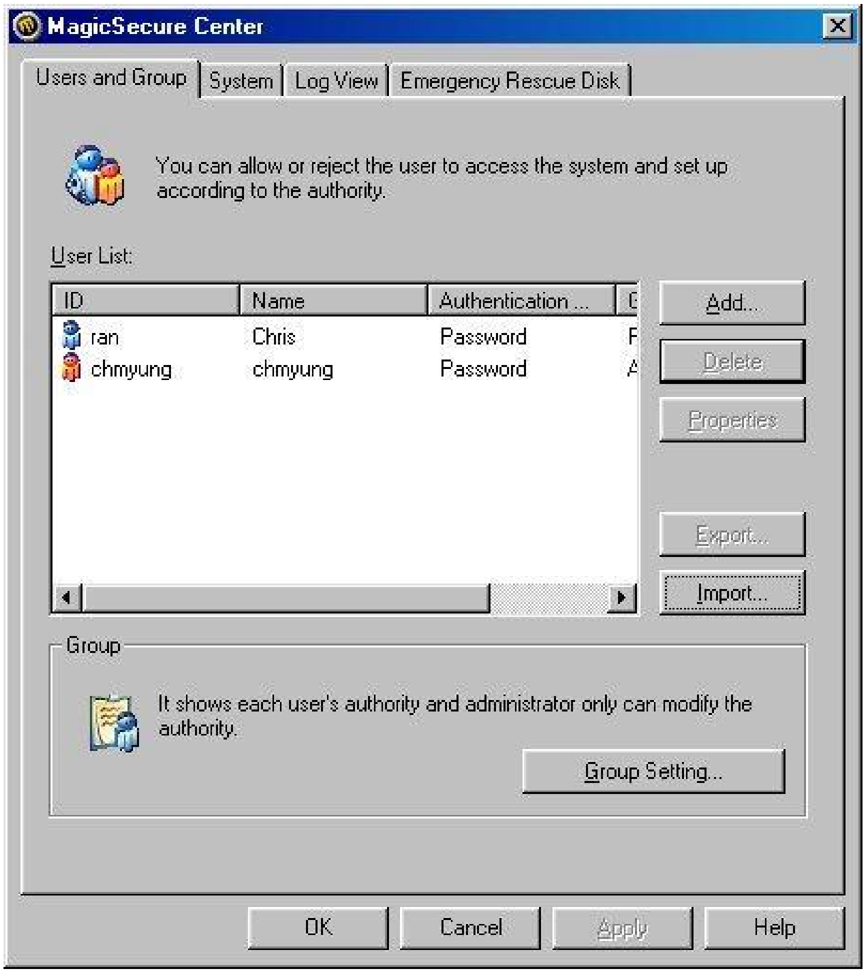
A message box will be displayed asking you to confirm whether you wish to delete the selected user. Click **Yes**.





Password : ******

Provide an administrator fingerprint/password to delete the user for good.



You can allow or reject the user to access the system and set up according to the authority.

User List:

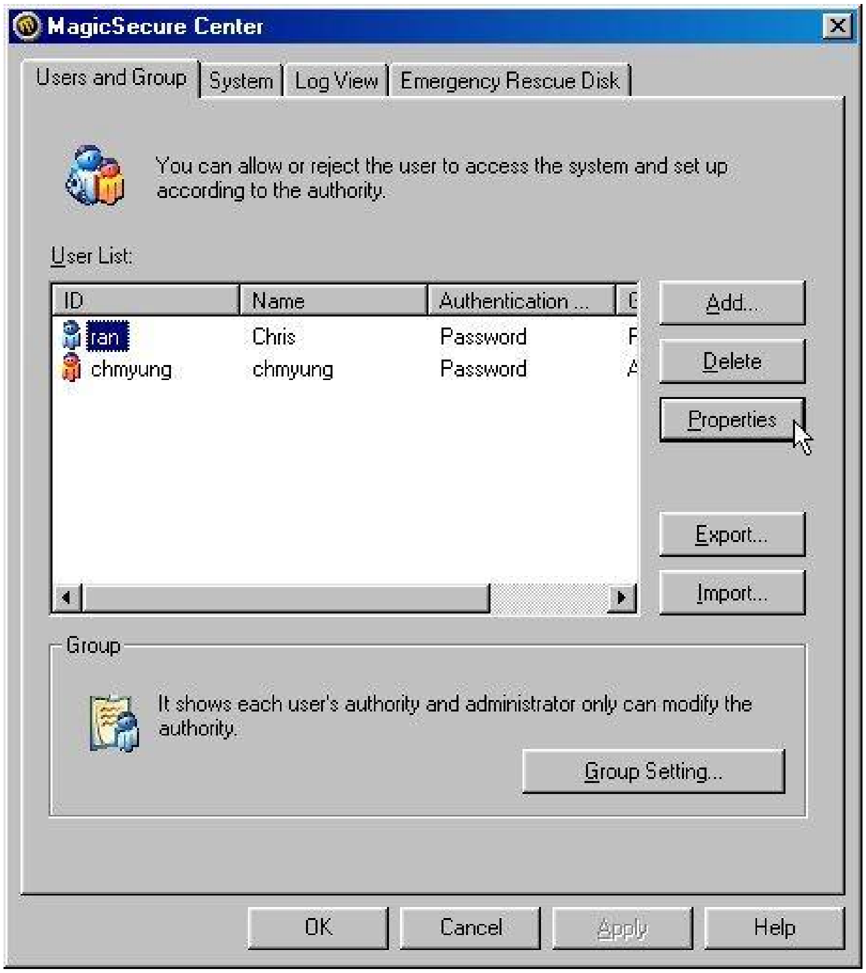
ID	Name	Authentication ...	[illegible]
ran	Chris	Password	F
chmyung	chmyung	Password	A

It shows each user's authority and administrator only can modify the authority.

In the example above, the user ‘tom’ has been deleted.

③ Properties

- You can change the user name, password and fingerprint(s). You can also modify the group the user belongs to as well as the identification type.
- You can change these settings from ‘Properties.’
- An administrator can change the group a user belongs to.

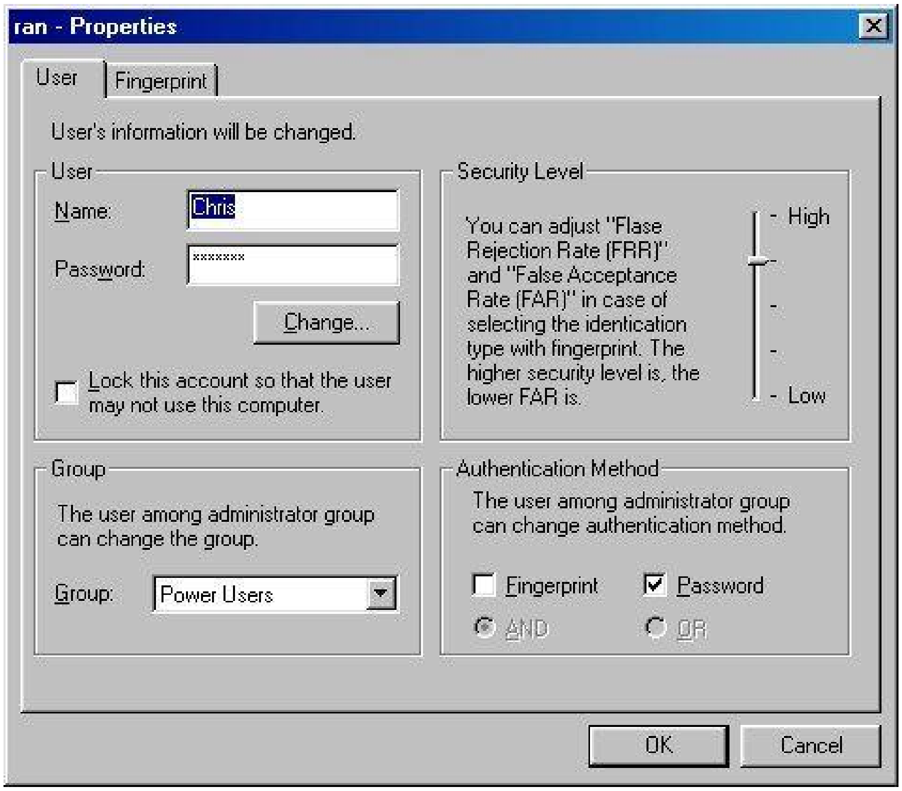


You can allow or reject the user to access the system and set up according to the authority.

ID	Name	Authentication ...	
ran	Chris	Password	F
chmyung	chmyung	Password	A

It shows each user's authority and administrator only can modify the authority.

In this example, the administrator selects the user ‘ran’ and clicks **Properties**.



User's information will be changed.

Name: Chris

Password: *******

☐ Lock this account so that the user may not use this computer.

You can adjust "Flase Rejection Rate (FRR)" and "False Acceptance Rate (FAR)" in case of selecting the identication type with fingerprint. The higher security level is, the lower FAR is.

The user among administrator group can change the group.

Group: Power Users

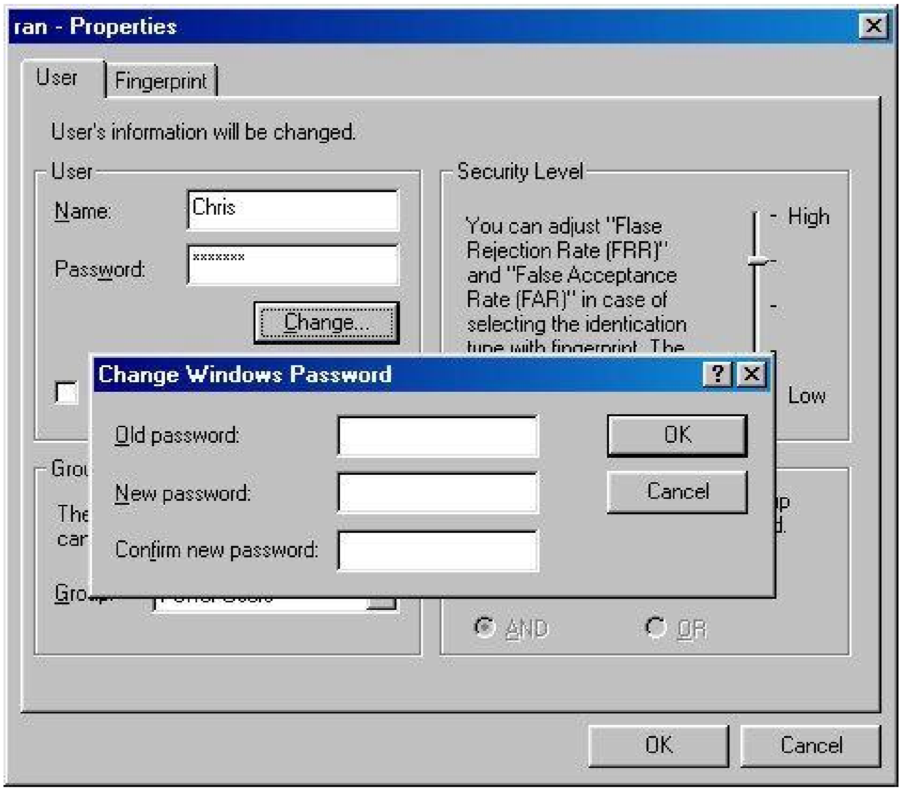
The user among administrator group can change authentication method.

☐ Fingerprint ☑ Password

● AND ○ OR

This is the **Properties** dialog box for 'ran'.

a. Changing user name and password



User's information will be changed.

Name: Chris

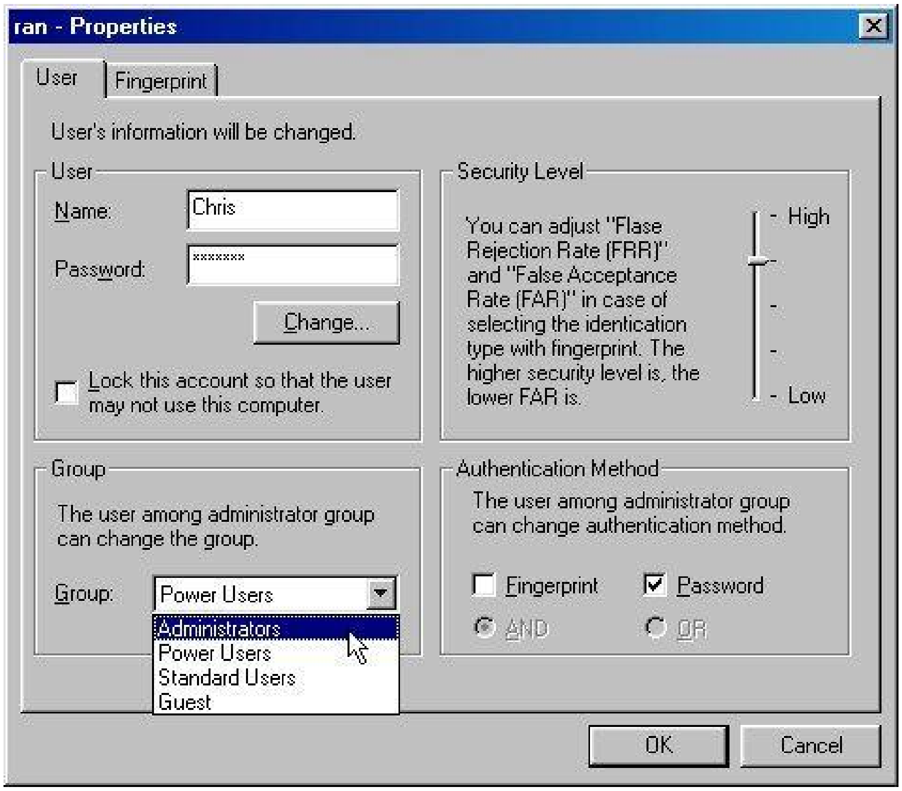
Password: *******

You can adjust "Flase Rejection Rate (FRR)" and "False Acceptance Rate (FAR)" in case of selecting the identication tune with fingerprint. The

Click **Change…** to modify the password.

b. Changing groups

Only an administrator can change a user’s group.



User's information will be changed.

Name: Chris

Password: *******

□ Lock this account so that the user may not use this computer.

You can adjust "Flase Rejection Rate (FRR)" and "False Acceptance Rate (FAR)" in case of selecting the identication type with fingerprint. The higher security level is, the lower FAR is.

The user among administrator group can change the group.

Group: Power Users

Administrators
Power Users
Standard Users
Guest

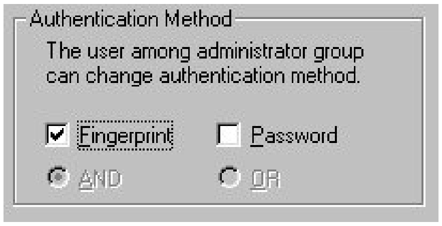
The user among administrator group can change authentication method.

□ Fingerprint ☑ Password

● AND ○ OR

You can change the group the selected user belongs to.

c. Change the **Authentication Method**



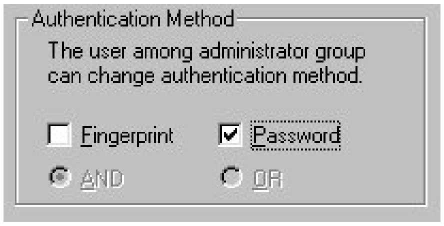
Authentication Method

The user among administrator group can change authentication method.

☑ Fingerprint □ Password

● AND ○ OR

Authentication with fingerprint only



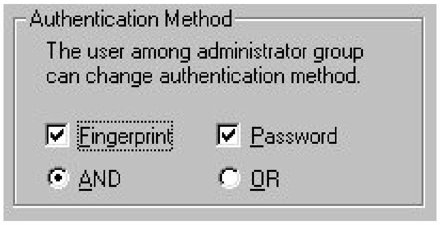
Authentication Method

The user among administrator group can change authentication method.

□ Fingerprint ☑ Password

● AND ○ OR

Authentication with password only

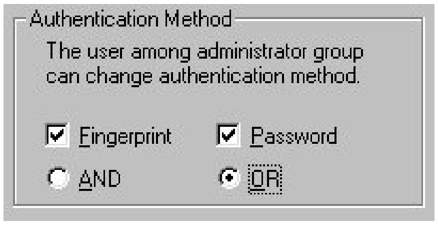


Authentication Method

The user among administrator group can change authentication method.

☑ Fingerprint ☑ Password

● AND ○ OR



Authentication Method

The user among administrator group can change authentication method.

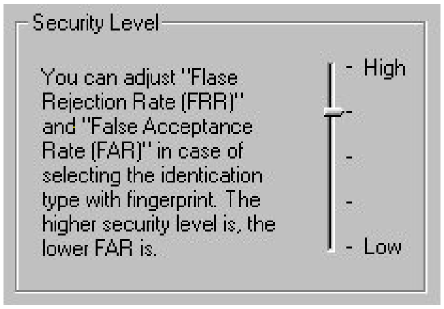
☑ Fingerprint ☑ Password

○ AND ● OR

Authentication with fingerprint AND password   Authentication with fingerprint OR password

d. Change the **Security Level**

- There are five security levels.
- Increasing the security level decreases the chance of unregistered fingerprints being incorrectly authenticated. (You should increase the security level if your fingerprint is vivid and has a high rate of successful authentication.)
- Decreasing the security level increases the chance of unregistered fingerprints being incorrectly authenticated. (You should decrease the security level if your fingerprint is not vivid or has a high rate of authentication failure.)

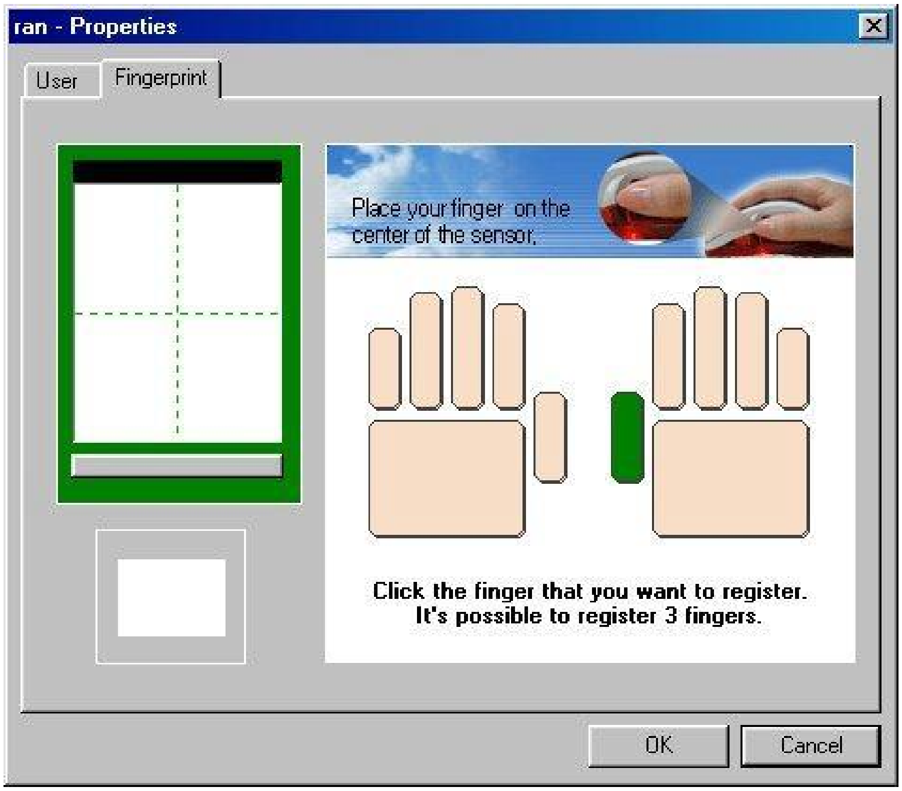


Security Level

You can adjust "Flase Rejection Rate (FRR)" and "False Acceptance Rate (FAR)" in case of selecting the identication type with fingerprint. The higher security level is, the lower FAR is.

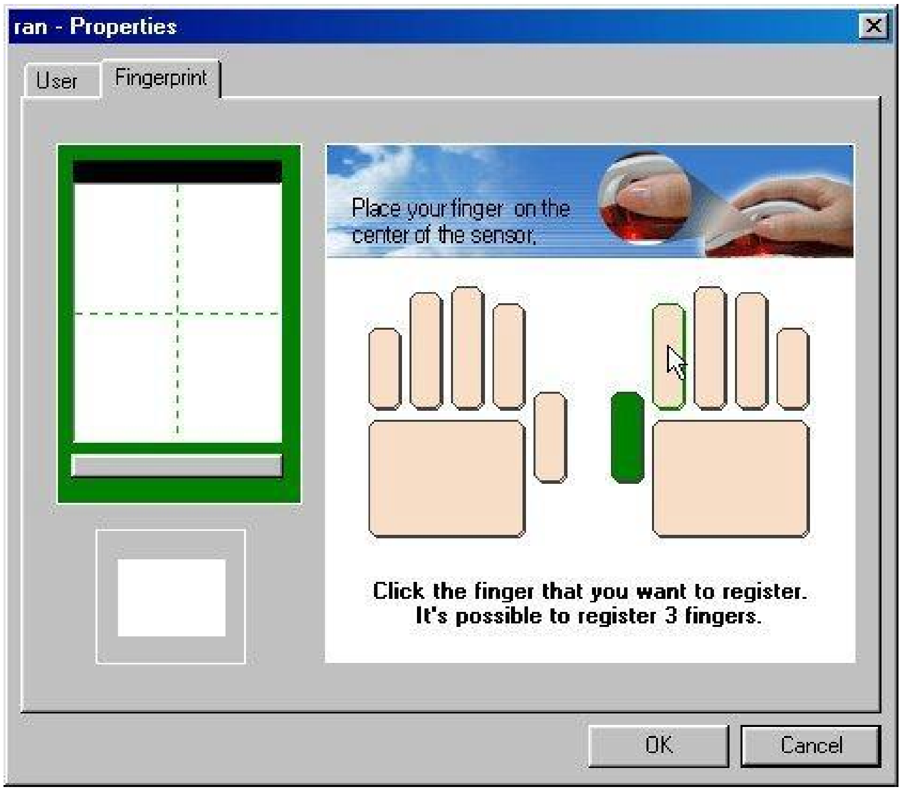
e. Register a fingerprint

- Click the finger you wish to register the print of and register your fingerprint.
- Up to three fingerprints can be registered per user.
- Please refer to the 'Add a user' section for a detailed description of the fingerprint registration procedure.



Click the finger that you want to register.
It's possible to register 3 fingers.

Before registering your fingerprint, click the finger you wish to register the print of.

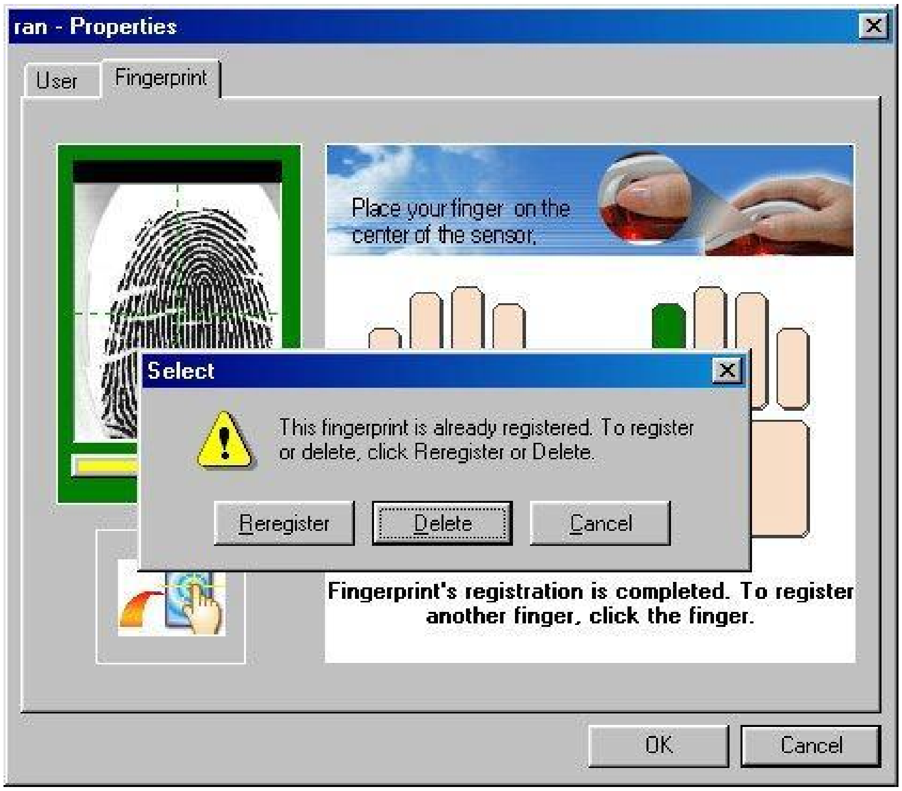


Click the finger that you want to register.
It's possible to register 3 fingers.

The figure above indicates that a fingerprint has been registered.

f. Delete a fingerprint

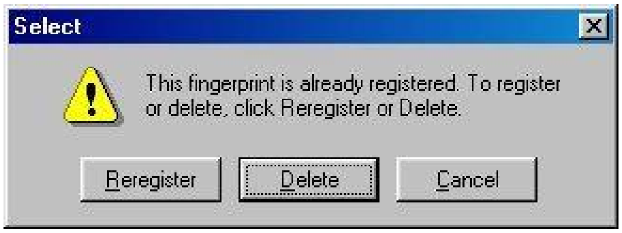
- A user must have at least one fingerprint registered. (i.e. The last fingerprint cannot be deleted)
- Click **Properties/Fingerprint Registration** and select the finger of the print that you wish to delete.



This fingerprint is already registered. To register or delete, click Reregister or Delete.

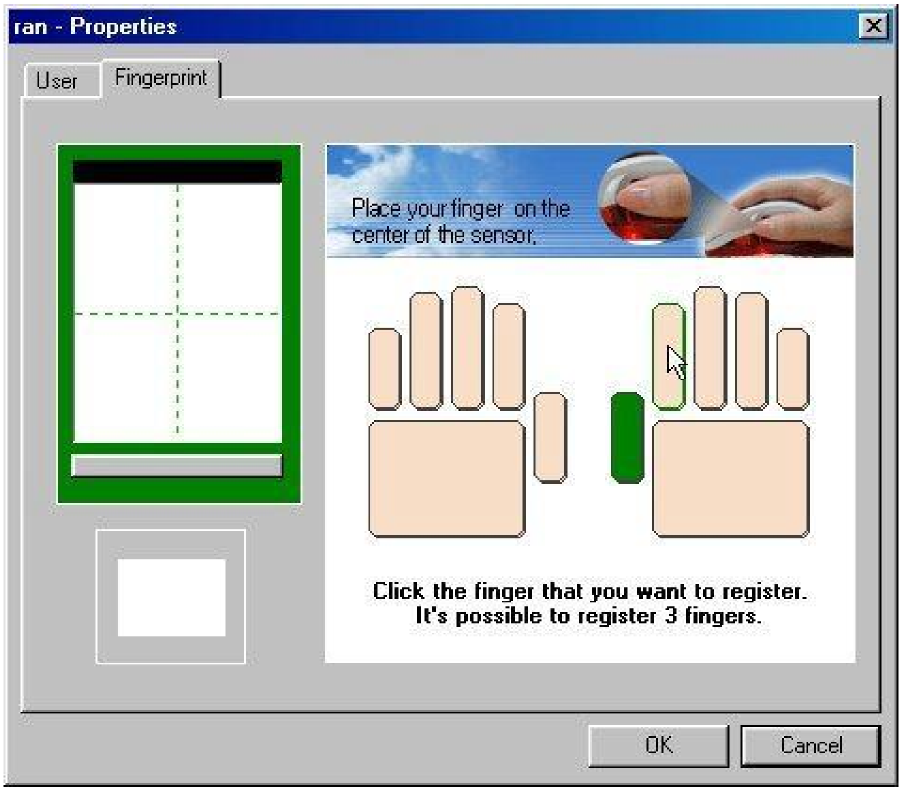
Fingerprint's registration is completed. To register another finger, click the finger.

The figure above displays a finger selected for fingerprint deletion.



This fingerprint is already registered. To register or delete, click Reregister or Delete.

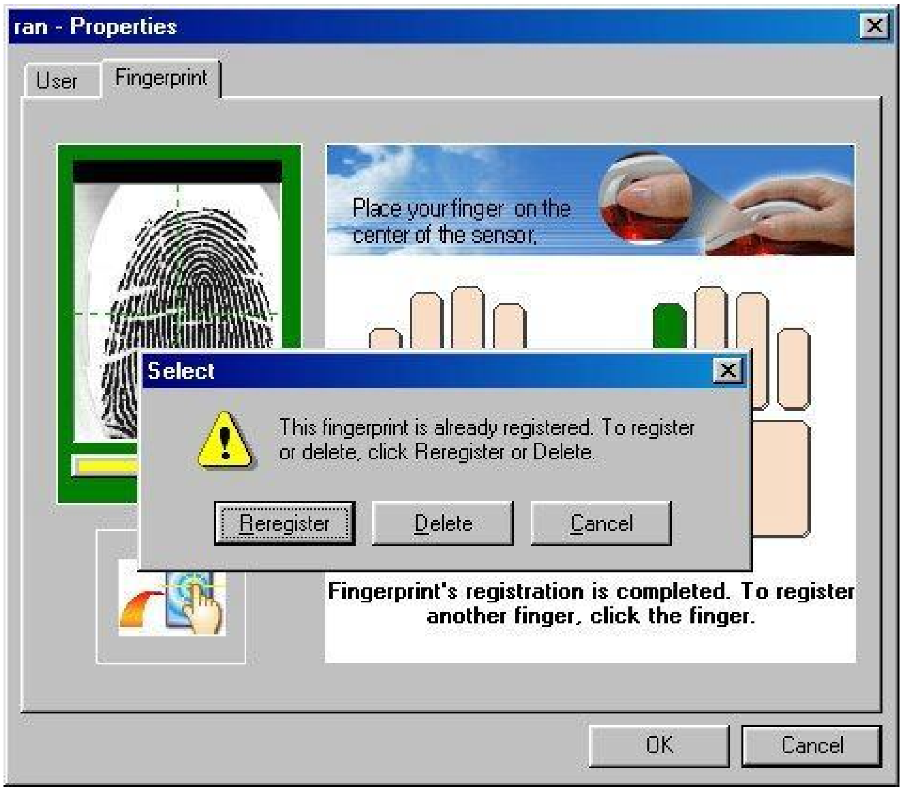
Click **Delete** button.


ran - Properties
User
Fingerprint
Place your finger on the center of the sensor.
Click the finger that you want to register.
It's possible to register 3 fingers.
OK
Cancel

The figure above displays the window after a fingerprint has been deleted.

g. Reregister a fingerprint

- Select **Properties/Reregister Fingerprint** and click the finger you wish to register the print of.

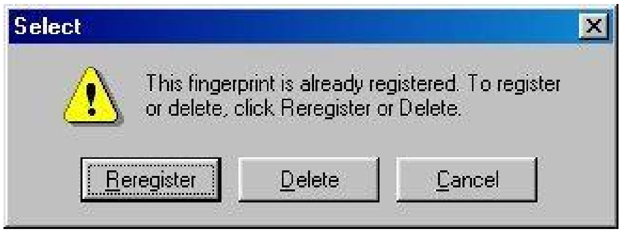


Place your finger on the center of the sensor.

This fingerprint is already registered. To register or delete, click Reregister or Delete.

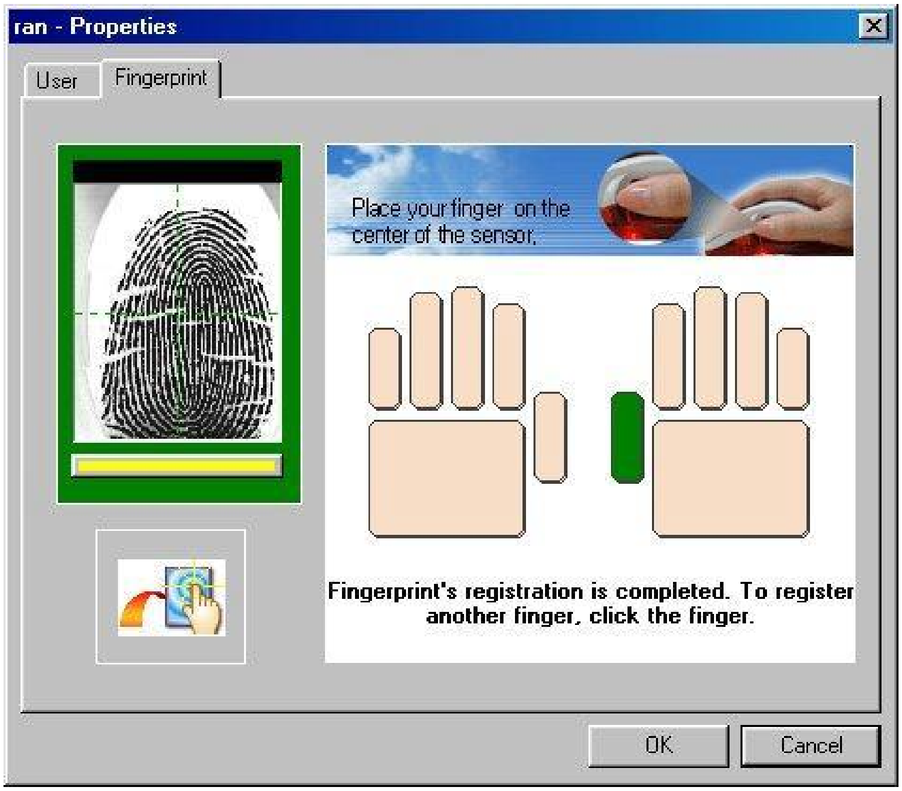
Fingerprint's registration is completed. To register another finger, click the finger.

The figure above displays a finger selected for reregistering a fingerprint.



This fingerprint is already registered. To register or delete, click Reregister or Delete.

Click **Reregister** button.



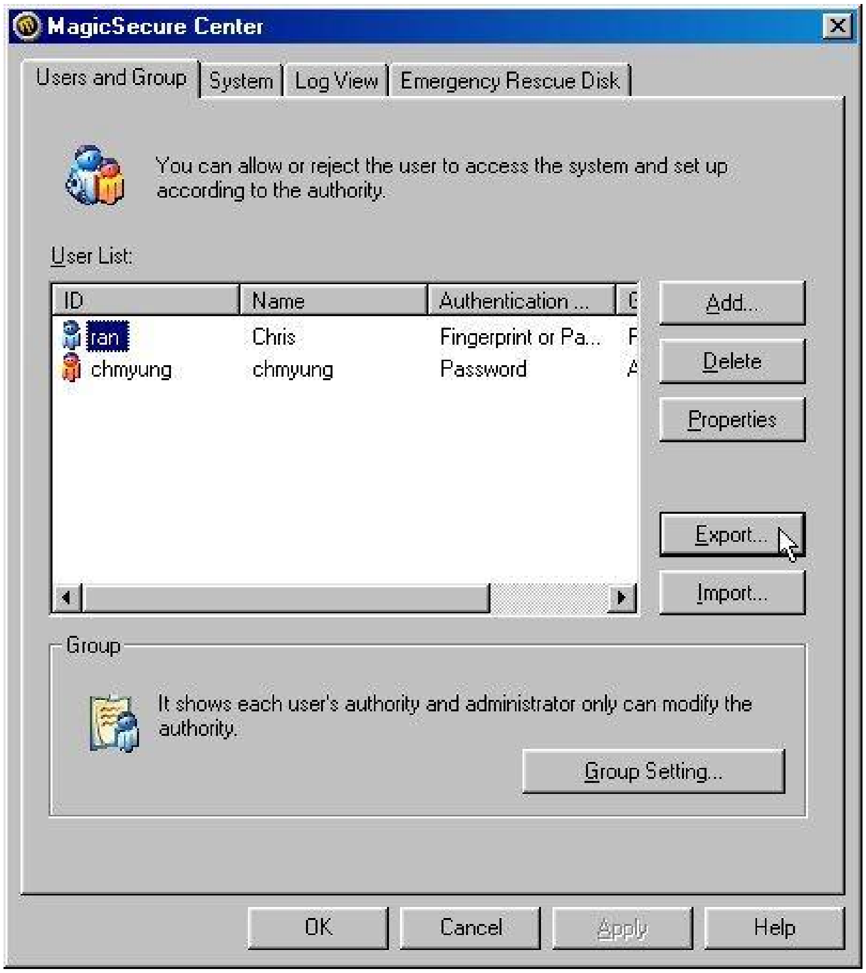
Place your finger on the center of the sensor.

Fingerprint's registration is completed. To register another finger, click the finger.

The figure above displays the window after reregistering a fingerprint.

④ **Export**

- You can backup users managed by the **Ramses II Center** as a file.
- The file will be saved with the extension *.mbk.
- The saved file will be encrypted to protect the user information.



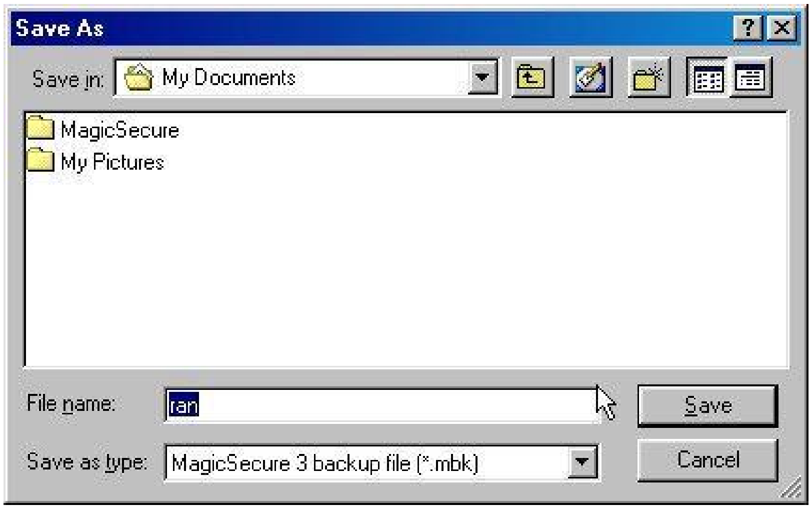
You can allow or reject the user to access the system and set up according to the authority.

User List:

ID	Name	Authentication ...	E
ran	Chris	Fingerprint or Pa...	F
chmyung	chmyung	Password	A

Group

It shows each user's authority and administrator only can modify the authority.



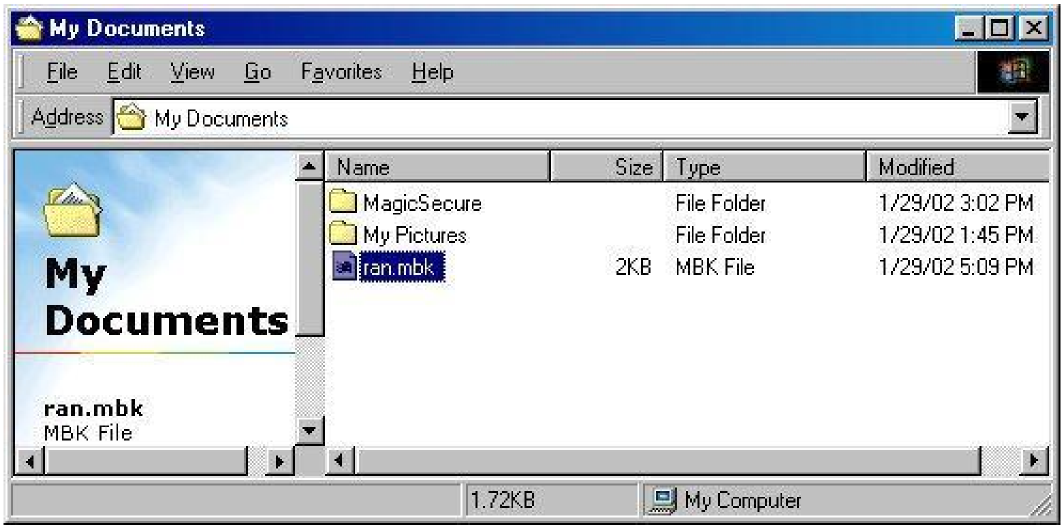
Save in: My Documents

MagicSecure
My Pictures

File name: ran

Save as type: MagicSecure 3 backup file (*.mbk)

Export selected users as a file (.mbk).



Address: My Documents

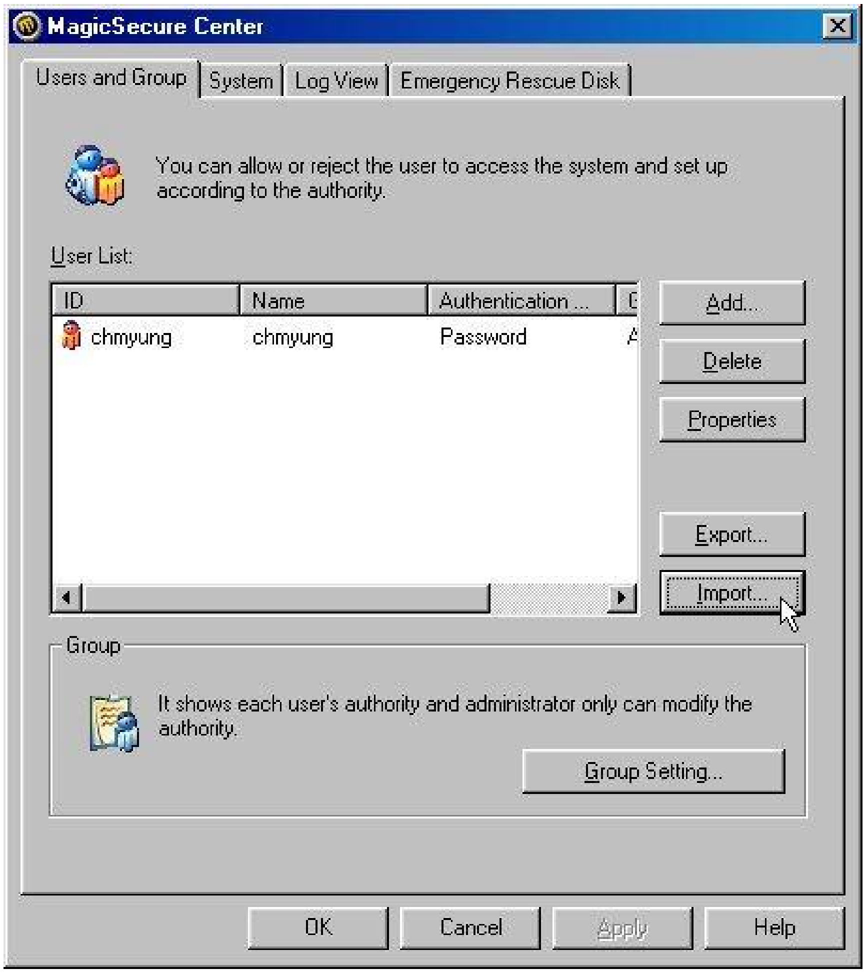
Name	Size	Type	Modified
MagicSecure		File Folder	1/29/02 3:02 PM
My Pictures		File Folder	1/29/02 1:45 PM
ran.mbk	2KB	MBK File	1/29/02 5:09 PM

In the example above, the file is saved as ran.mbk.

⑤ **Import**

- Users backed up from the **Ramses II Center** can be added to **Users and Group**.
- Import the *.mbk file.

* If the user does not exist in the list

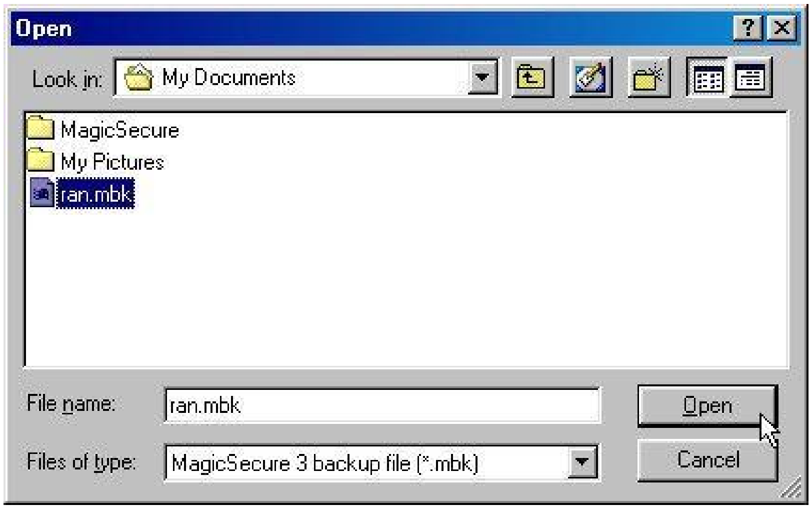


You can allow or reject the user to access the system and set up according to the authority.

User List:

ID	Name	Authentication ...
chmyung	chmyung	Password

It shows each user's authority and administrator only can modify the authority.



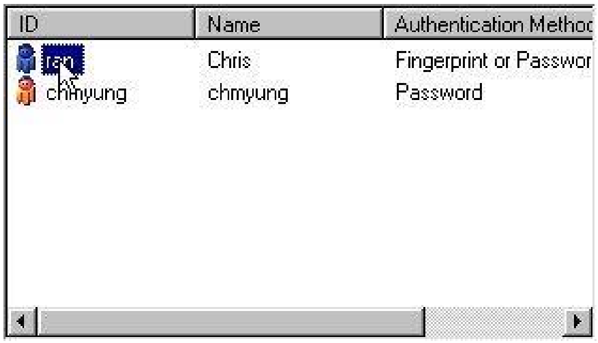
Look in: My Documents

- MagicSecure
- My Pictures
- ran.mbk

File name: ran.mbk

Files of type: MagicSecure 3 backup file (*.mbk)

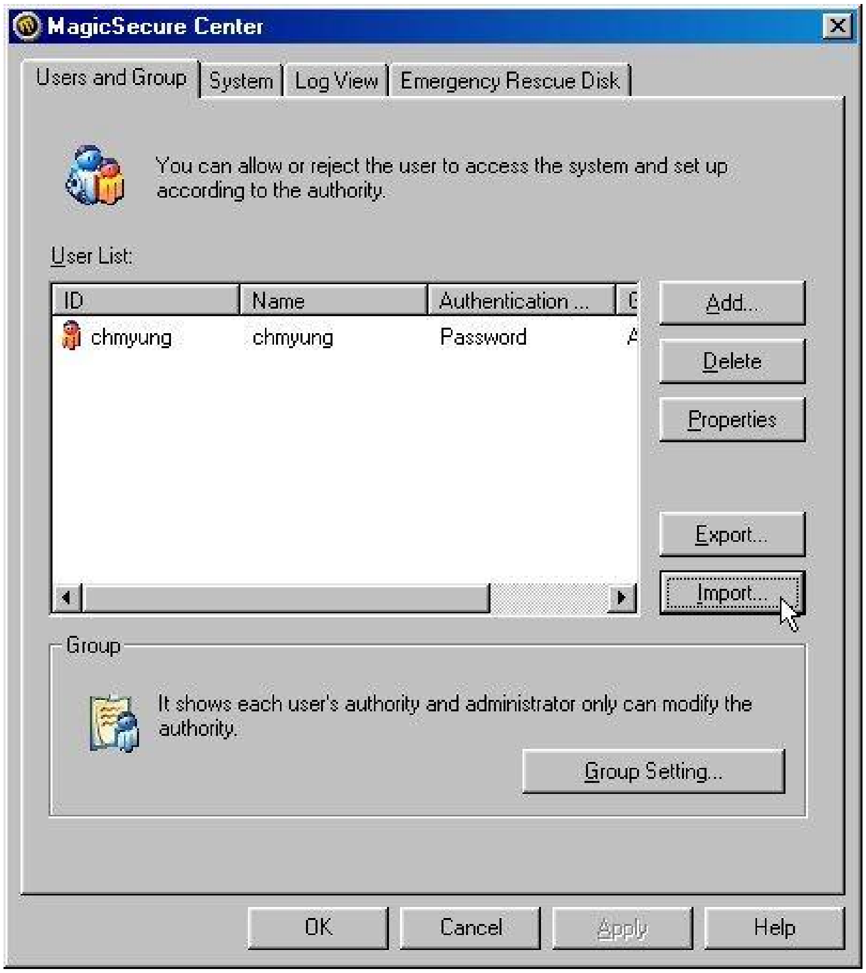
Import the user from the file. (ran.mbk in this example)



ID	Name	Authentication Methoc
ran	Chris	Fingerprint or Passwor
chmyung	chmyung	Password

The figure above displays the user ‘ran’ added to the list from the backup file.

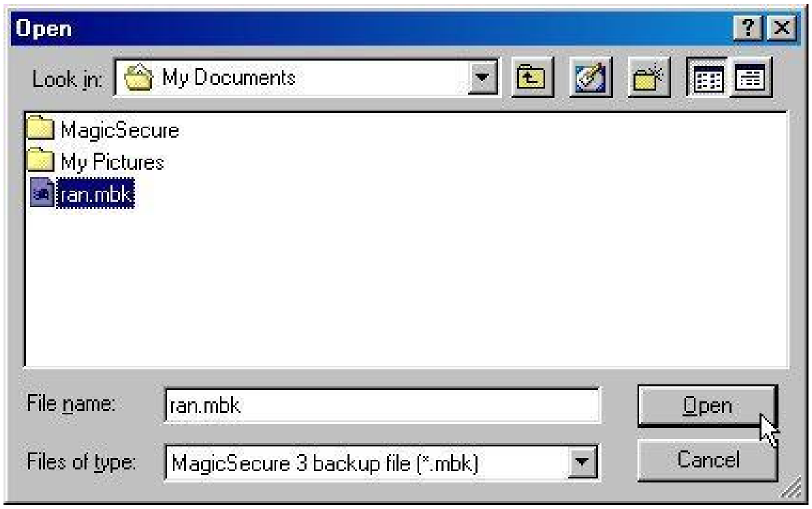
* If the user already exists in the list



You can allow or reject the user to access the system and set up according to the authority.

ID	Name	Authentication ...	C
chmyung	chmyung	Password	A

It shows each user's authority and administrator only can modify the authority.

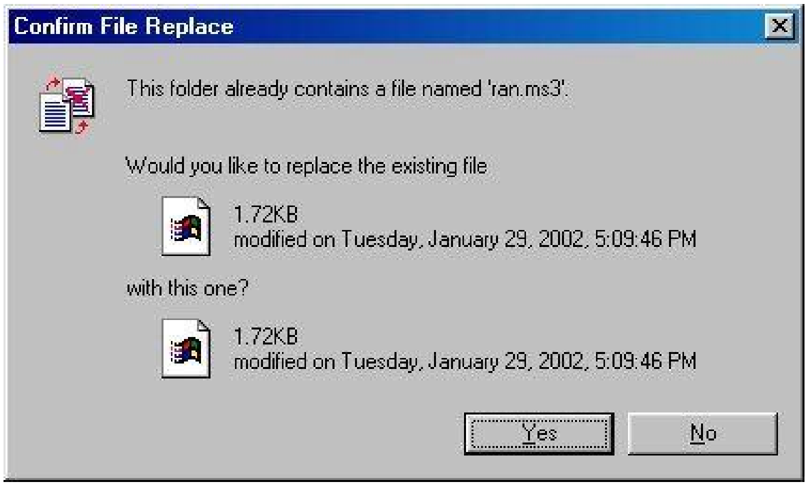


Look in: My Documents

File name: ran.mbk

Files of type: MagicSecure 3 backup file (*.mbk)

Import the user from the file. (ran.mbk in this example)


Confirm File Replace

This folder already contains a file named 'ran.ms3'.

Would you like to replace the existing file

1.72KB
modified on Tuesday, January 29, 2002, 5:09:46 PM

with this one?

1.72KB
modified on Tuesday, January 29, 2002, 5:09:46 PM

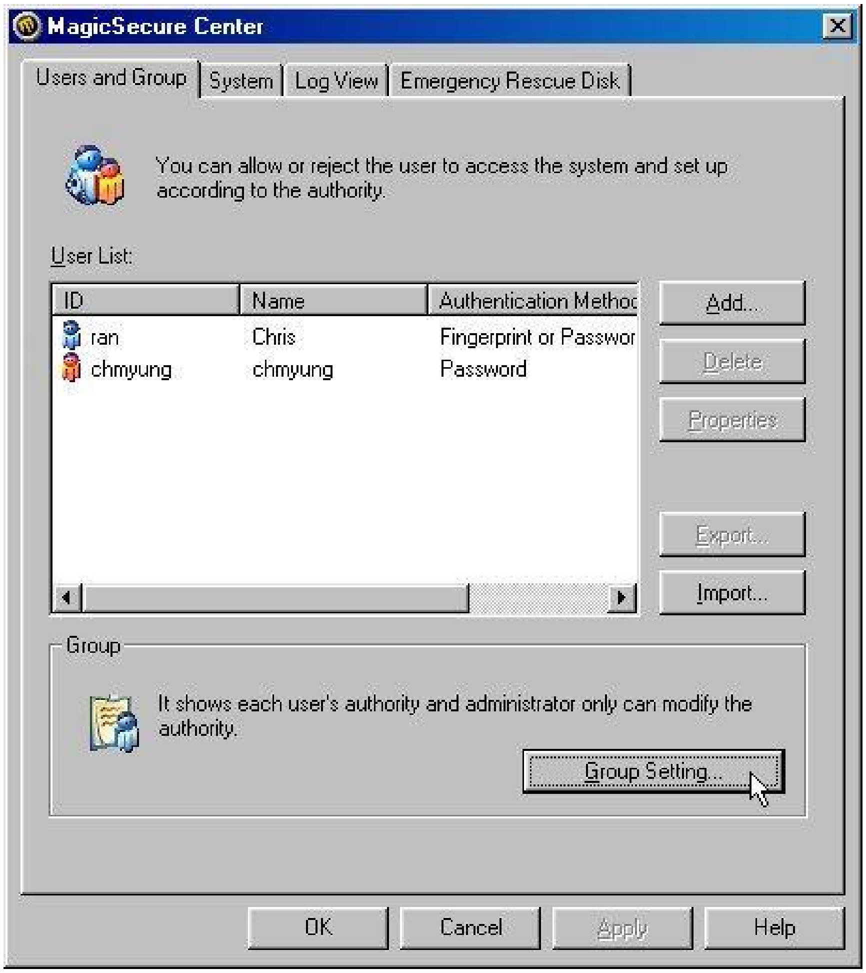
Since the user already exists in the list, click **Yes** to overwrite the existing data.

⑥ Setting Group/User Authorities

- Default settings
- Only an administrator can set group/user authorities

Group Authority	Administrator	Super User	Standard User
Select Logon Method	O	O	X
My SecureDocs Management	O	O	O
Register User	O	X	X
Delete User	O	X	X
View or Modify User Information	O	O	X
View or Modify One's Own Information	O	O	O
Import/Export User	O	O	X
View/Print/Import Log File	O	O	X
Set Security Level	O	O	O
Install/Remove Boot Protection	O	X	X
Set Boot Control Key	O	X	X
Set Encryption Algorithm	O	X	X
Test Fingerprint Sensor	O	X	X
Emergency Rescue Disk	O	X	X
System Restoration	O	X	X
Remove Ramses II ver 3.0	O	X	X

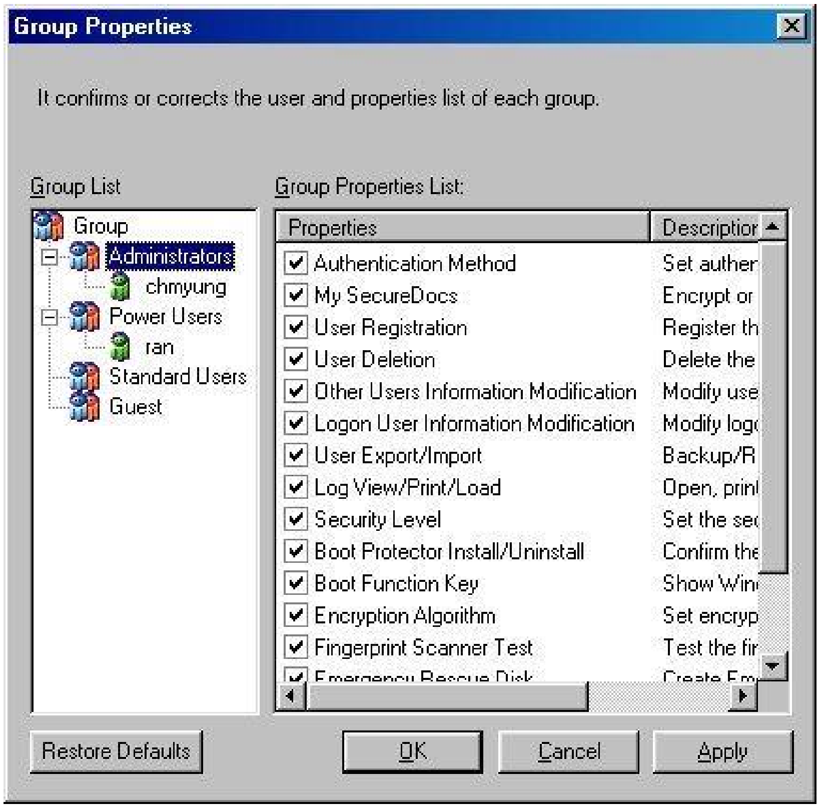
※ A 'Guest' does not have any authority under default settings.



You can allow or reject the user to access the system and set up according to the authority.

ID	Name	Authentication Methoc
ran	Chris	Fingerprint or Passwor
chmyung	chmyung	Password

It shows each user's authority and administrator only can modify the authority.



Group Properties

It confirms or corrects the user and properties list of each group.

Group List

- Group
  - Administrators
    - chmyung
  - Power Users
    - ran
  - Standard Users
  - Guest

Group Properties List:

Properties	Descriptior
☑ Authentication Method	Set auther
☑ My SecureDocs	Encrypt or
☑ User Registration	Register th
☑ User Deletion	Delete the
☑ Other Users Information Modification	Modify use
☑ Logon User Information Modification	Modify logo
☑ User Export/Import	Backup/R
☑ Log View/Print/Load	Open, prin
☑ Security Level	Set the se
☑ Boot Protector Install/Uninstall	Confirm the
☑ Boot Function Key	Show Win
☑ Encryption Algorithm	Set encryp
☑ Fingerprint Scanner Test	Test the fir
☑ Emergency Rescue Disk	Create Em

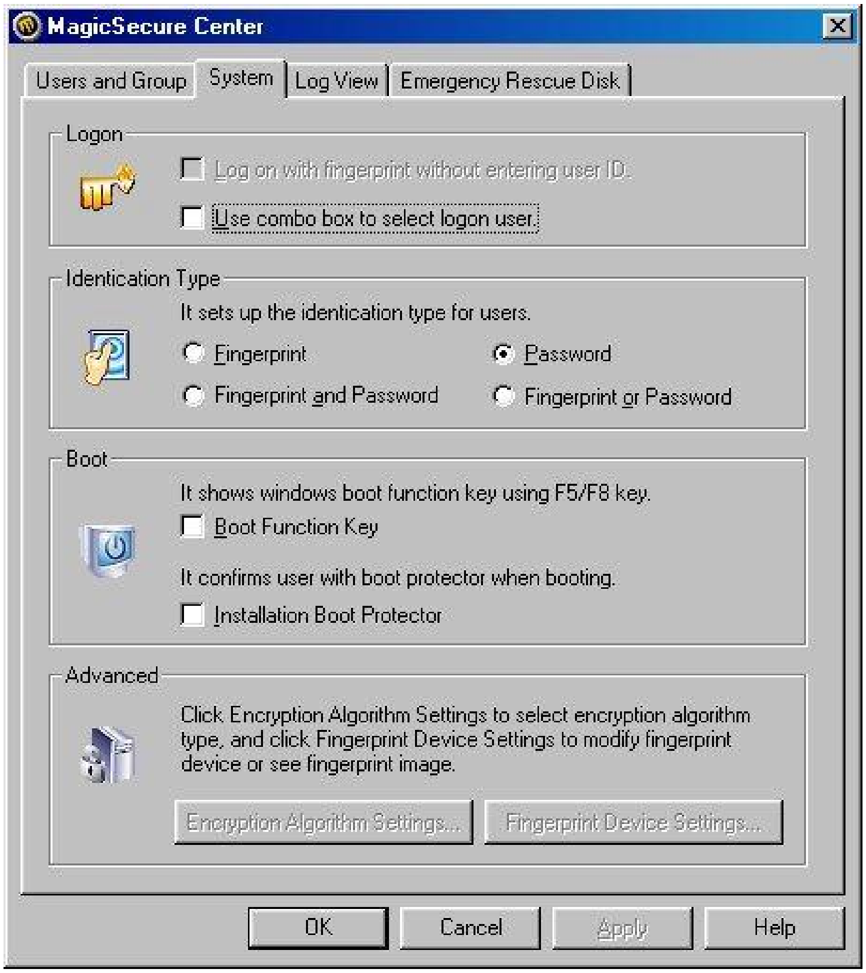
The figure above displays the window for setting user/group authorities.

You can select or deselect authorities from the **Group Properties** list.

(3) System Configuration

With the exception of Logon, only an administrator can change system configuration settings.

- Logon: You can change the logon window display according to the logon method.
- Identification Type: The standard user authentication method can be configured from the group settings.
- Boot Control: F5/F8 keys can be disabled to prevent files from being modified after safe mode booting, etc.



Logon

☐ Log on with fingerprint without entering user ID.

☐ Use combo box to select logon user.

Identication Type

It sets up the identication type for users.

○ Fingerprint ● Password

○ Fingerprint and Password ○ Fingerprint or Password

Boot

It shows windows boot function key using F5/F8 key.

☐ Boot Function Key

It confirms user with boot protector when booting.

☐ Installation Boot Protector

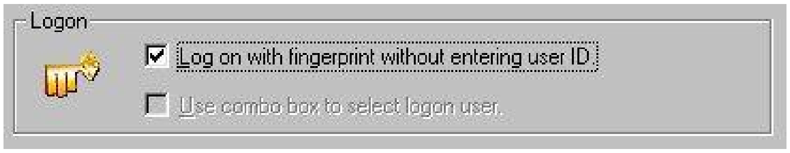
Advanced

Click Encryption Algorithm Settings to select encryption algorithm type, and click Fingerprint Device Settings to modify fingerprint device or see fingerprint image.

Encryption Algorithm Settings...
Fingerprint Device Settings...
OK
Cancel
Apply
Help

Select the **System** tab from the **Ramses II Center**.

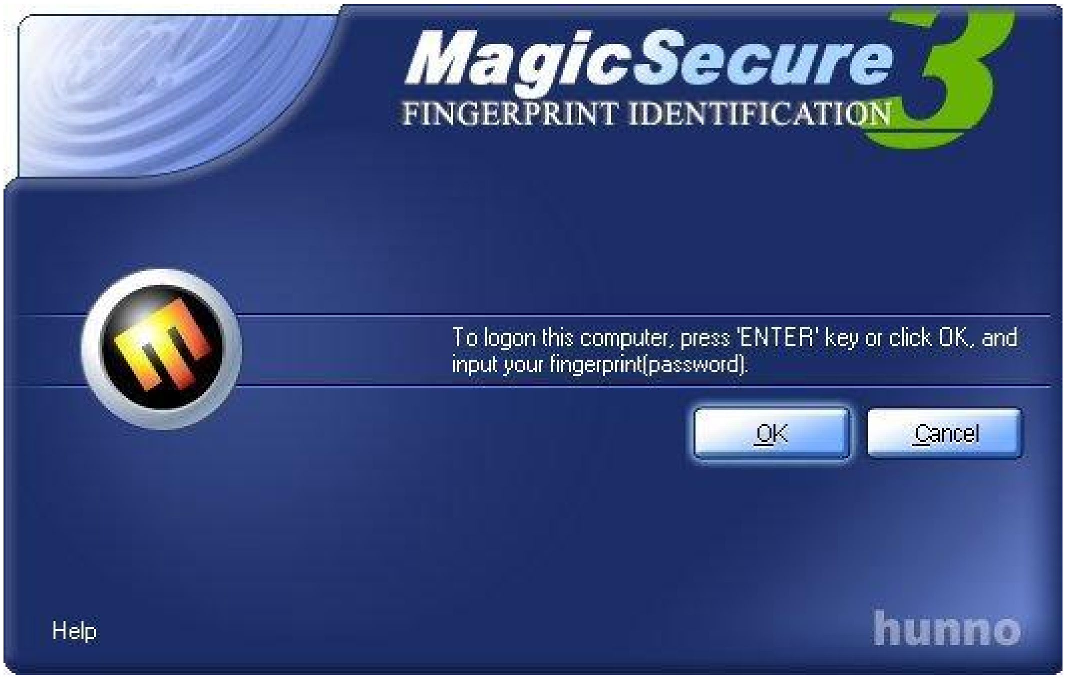
You can change system settings such as the Identification Type, boot control and encryption.



Logon

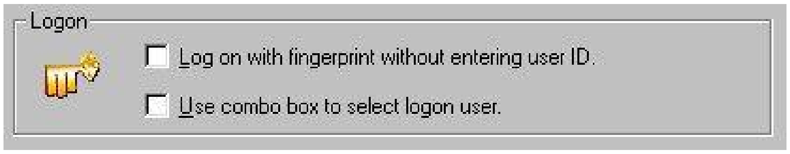
☑ Log on with fingerprint without entering user ID.

□ Use combo box to select logon user.



To logon this computer, press 'ENTER' key or click OK, and input your fingerprint(password).

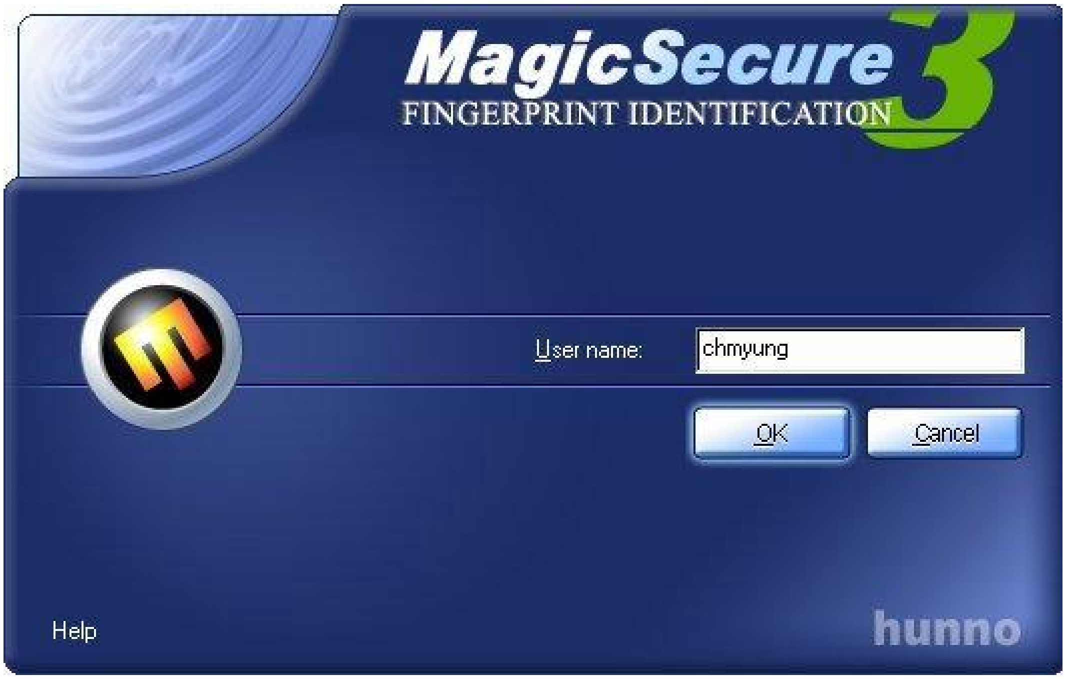
The user name is not displayed during the logon procedure.



Logon

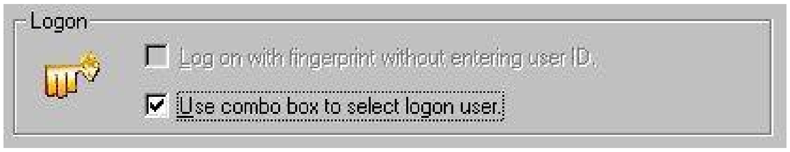
□ Log on with fingerprint without entering user ID.

□ Use combo box to select logon user.



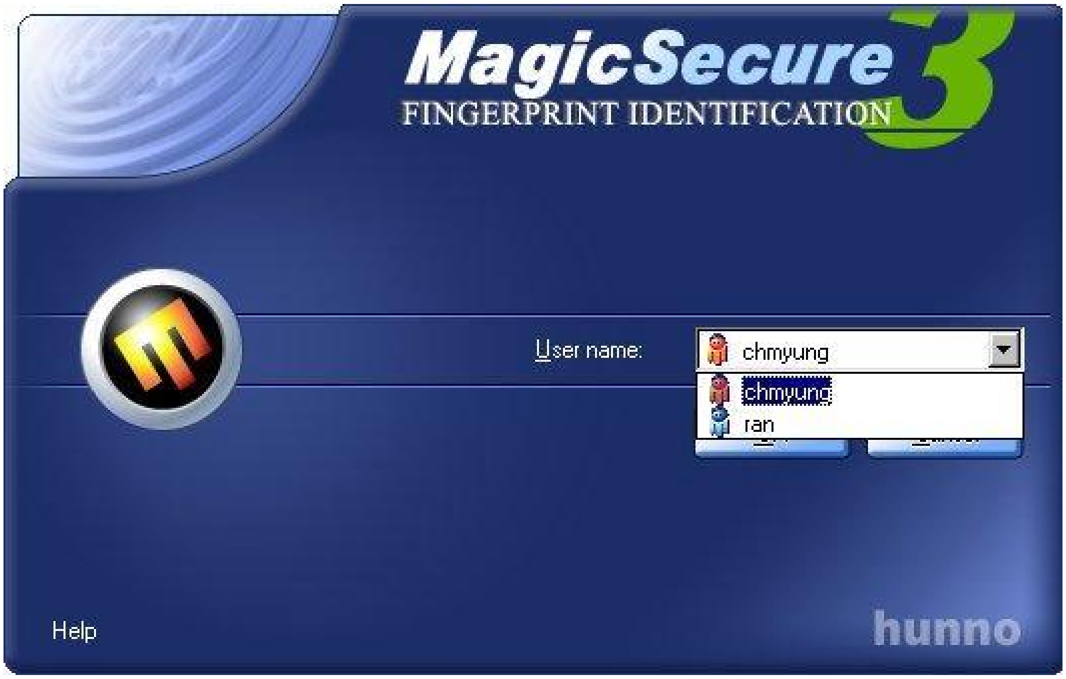
User name: chmyung

The user name is displayed during the logon procedure.

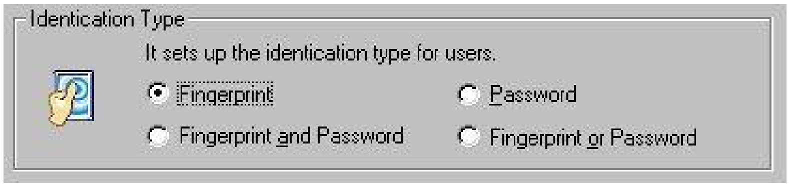

Logon

□ Log on with fingerprint without entering user ID.

☑ Use combo box to select logon user.



User names are displayed in a combo box during the logon procedure.



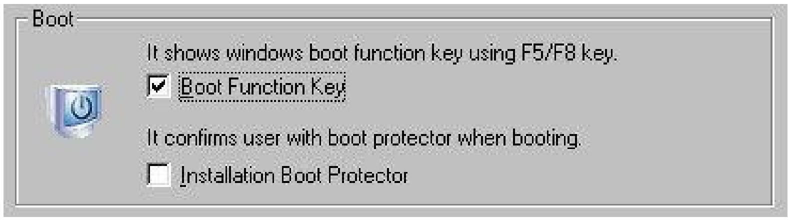
Identication Type

It sets up the identication type for users.

● Fingerprint ○ Password

○ Fingerprint and Password ○ Fingerprint or Password

Select the **Identification Type**.



Boot

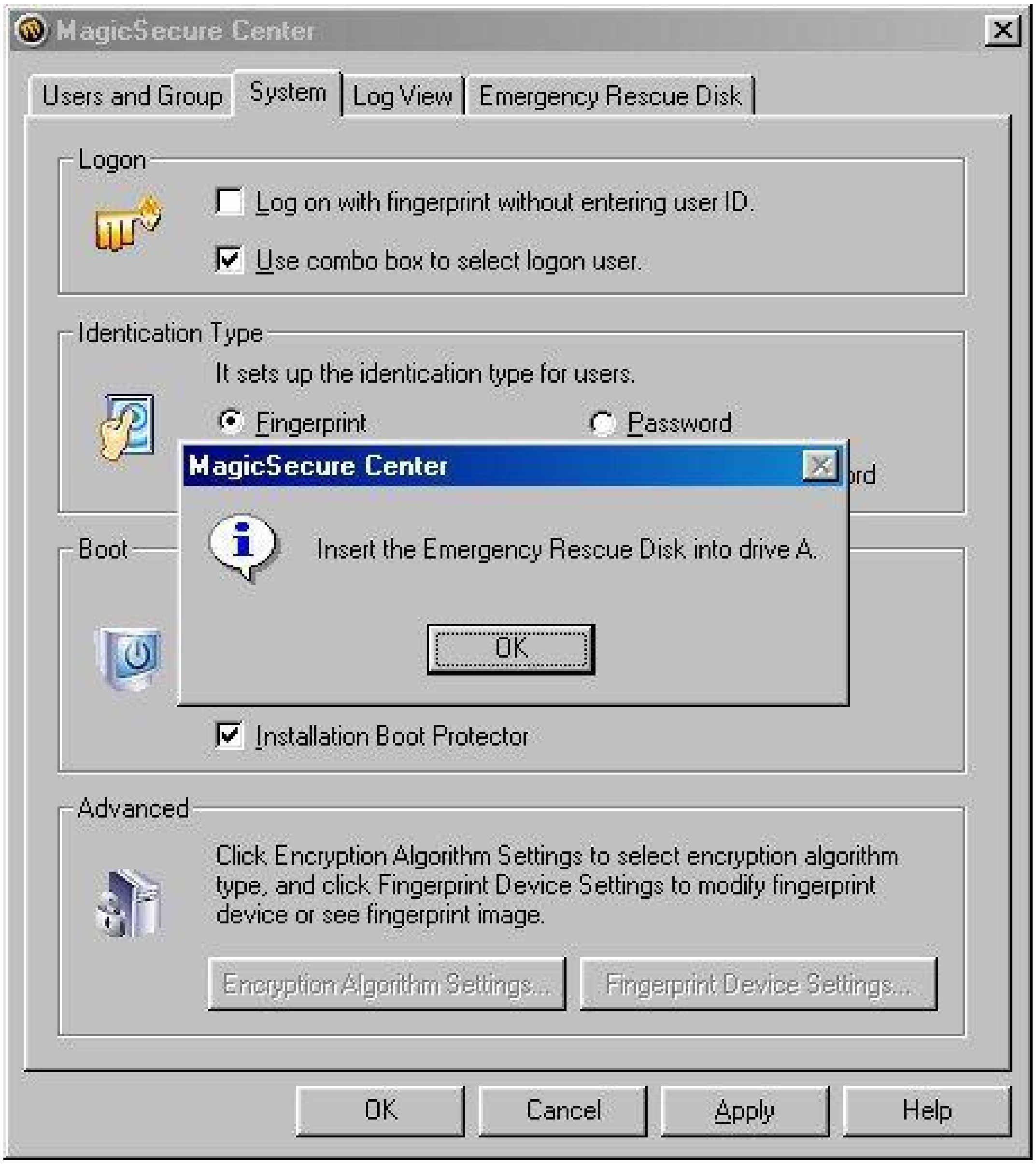
It shows windows boot function key using F5/F8 key.

☑ Boot Function Key

It confirms user with boot protector when booting.

□ Installation Boot Protector

Select this option to prevent file access after booting the system in the safe or DOS mode.



☐ Log on with fingerprint without entering user ID.

☑ Use combo box to select logon user.

It sets up the identication type for users.

● Fingerprint ○ Password

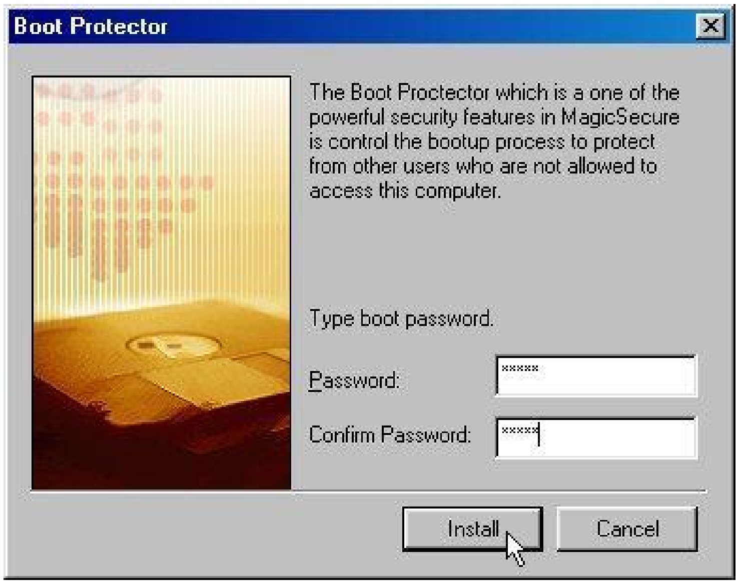
☑ Installation Boot Protector

Click Encryption Algorithm Settings to select encryption algorithm type, and click Fingerprint Device Settings to modify fingerprint device or see fingerprint image.

MagicSecure Center

Insert the Emergency Rescue Disk into drive A.

If you wish to use the **Boot Protector**, check the option, insert the Emergency Rescue Disk in drive A: and then click **OK**.



Boot Protector

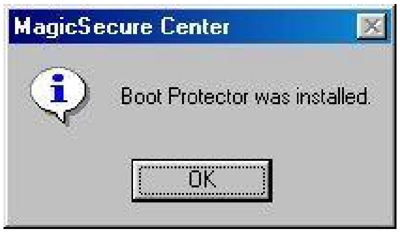
The Boot Proctector which is a one of the powerful security features in MagicSecure is control the bootup process to protect from other users who are not allowed to access this computer.

Type boot password.

Password: *****

Confirm Password: *****

Input the Emergency Rescue Disk password and click **Install**.



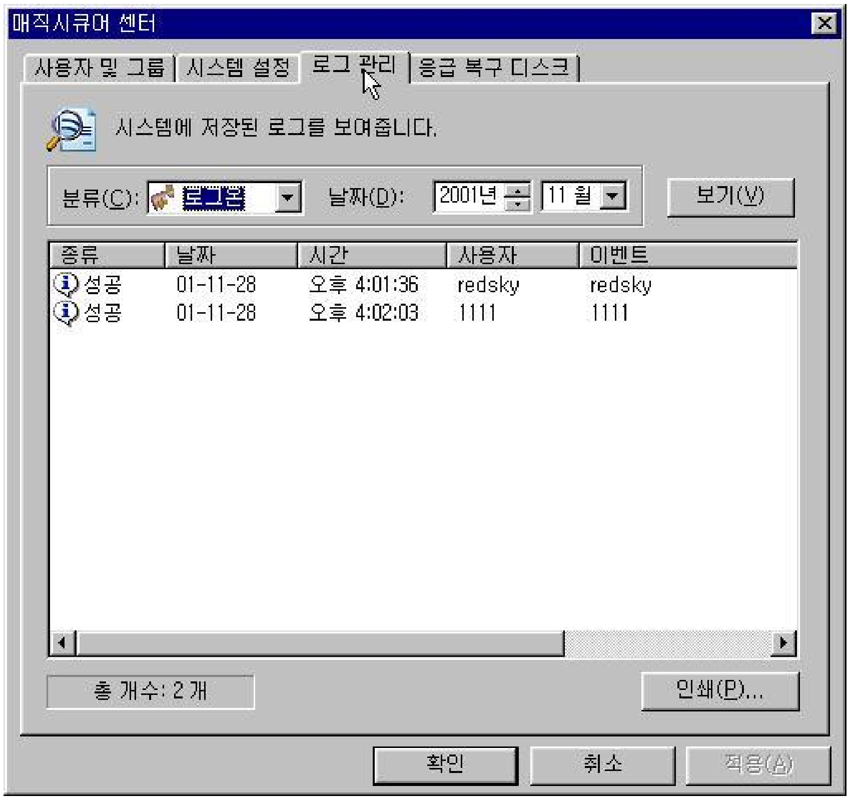
MagicSecure Center

Boot Protector was installed.

A message will be displayed indicating the Boot Protector is successfully installed. Click **OK**.

(4) Log Management

- You can view the log files generated by date.
- You can view the log file content according to each category. (logon, user, encryption, system)
- You can check and print the log file for each date.



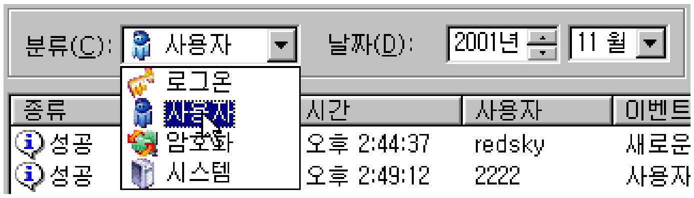
시스템에 저장된 로그를 보여줍니다.

분류(C): 로그온 날짜(D): 2001년 11 월

종류	날짜	시간	사용자	이벤트
성공	01-11-28	오후 4:01:36	redsky	redsky
성공	01-11-28	오후 4:02:03	1111	1111

총 개수: 2 개

The figure above displays the **Log Management** screen.



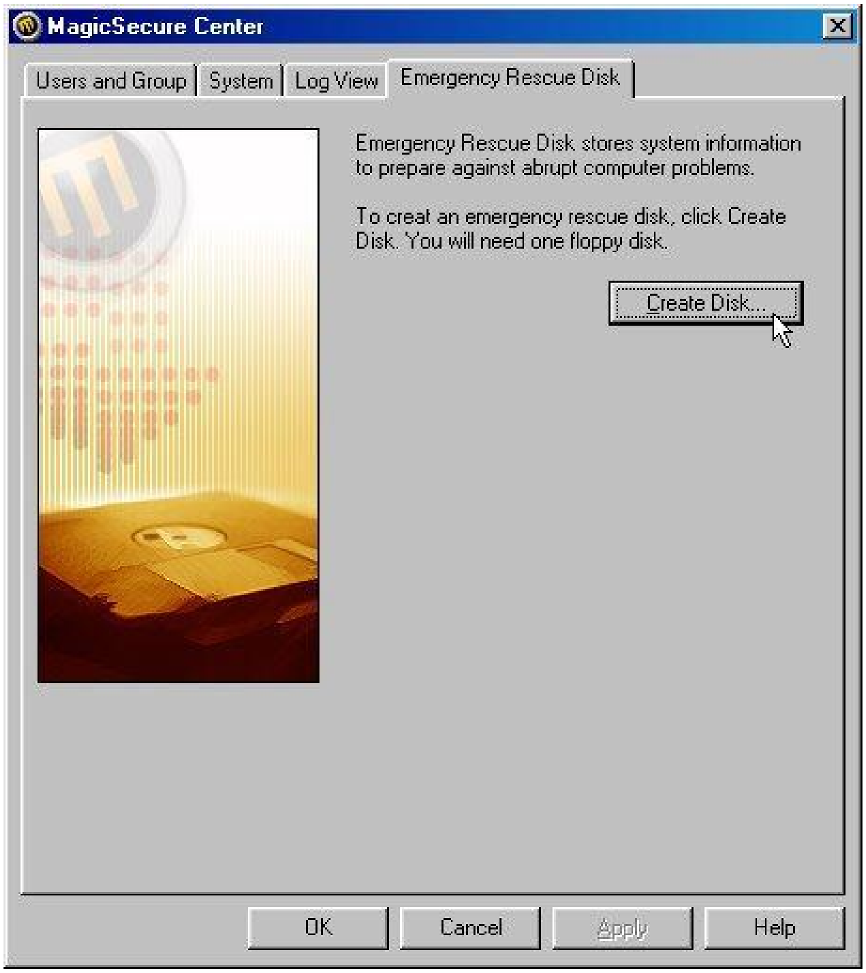
분류(C): 사용자 날짜(D): 2001년 11 월

종류	시간	사용자	이벤트
성공	오후 2:44:37	redsky	새로운
성공	오후 2:49:12	2222	사용자

You can view categorical logs by selecting from the combo box.

(5) Emergency Rescue Disk

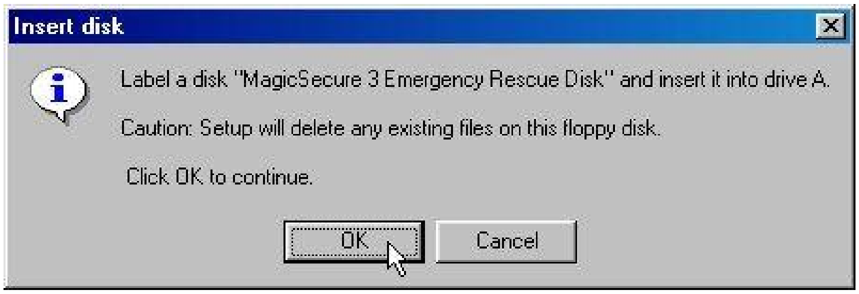
- You can use ‘sysback.exe’ to restore the system configuration to the point when the **Emergency Rescue Disk** was created.



Emergency Rescue Disk stores system information to prepare against abrupt computer problems.

To creat an emergency rescue disk, click Create Disk. You will need one floppy disk.

Select the **Emergency Rescue Disk** tab and click **Create Disk…**.



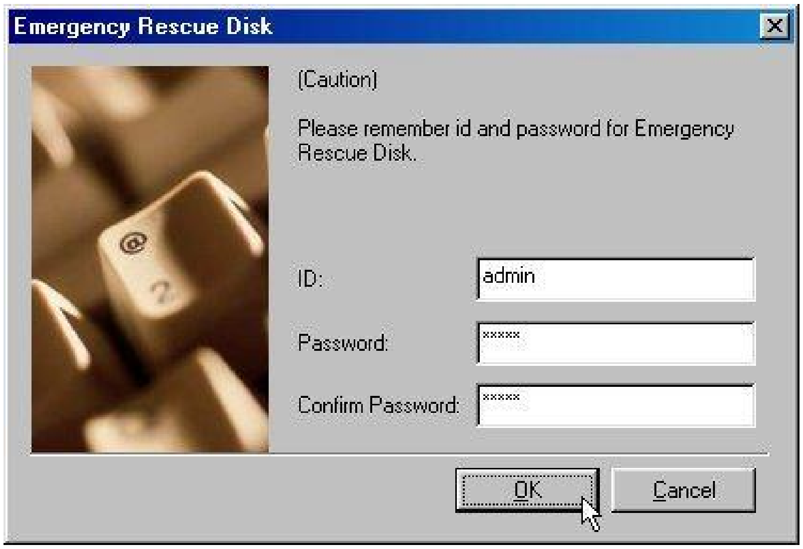
Insert disk

Label a disk "MagicSecure 3 Emergency Rescue Disk" and insert it into drive A.

Caution: Setup will delete any existing files on this floppy disk.

Click OK to continue.

Insert a blank floppy disk in drive A: and click **OK**.



Emergency Rescue Disk

(Caution)

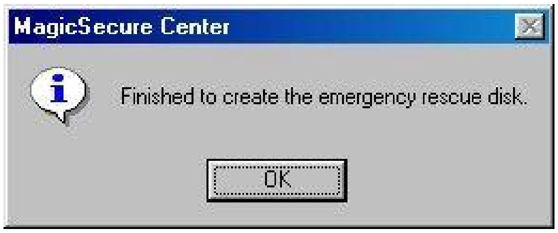
Please remember id and password for Emergency Rescue Disk.

ID: admin

Password: *****

Confirm Password: *****

Input an ID and password for the Emergency Rescue Disk. (You can provide a random ID and password at your discretion)

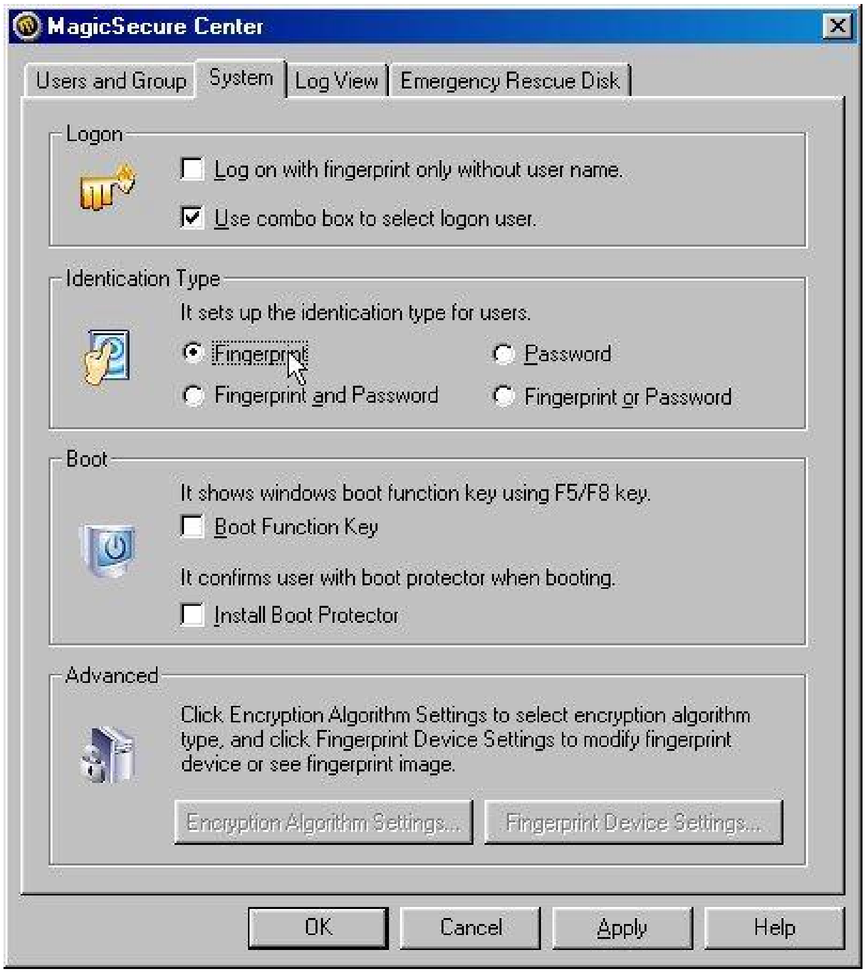


MagicSecure Center

Finished to create the emergency rescue disk.

A message will be displayed indicating that the emergency rescue disk is successfully created. Click **OK**.

How to recover the system configuration and after modification



Logon

☐ Log on with fingerprint only without user name.

☑ Use combo box to select logon user.

Identication Type

It sets up the identication type for users.

● Fingerprint ○ Password

○ Fingerprint and Password ○ Fingerprint or Password

Boot

It shows windows boot function key using F5/F8 key.

☐ Boot Function Key

It confirms user with boot protector when booting.

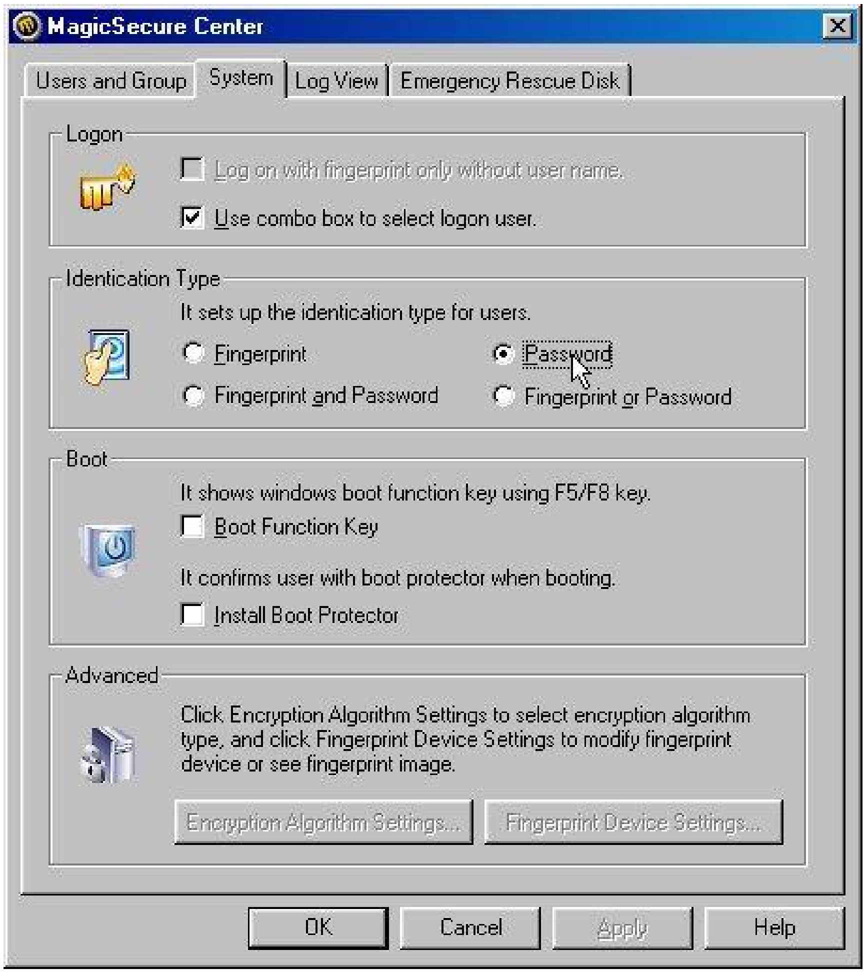
☐ Install Boot Protector

Advanced

Click Encryption Algorithm Settings to select encryption algorithm type, and click Fingerprint Device Settings to modify fingerprint device or see fingerprint image.

Encryption Algorithm Settings...
Fingerprint Device Settings...
OK
Cancel
Apply
Help

The figure above displays the system configuration right before the Emergency Rescue Disk is created.



Logon

☐ Log on with fingerprint only without user name.

☑ Use combo box to select logon user.

Identication Type

It sets up the identication type for users.

○ Fingerprint ● Password

○ Fingerprint and Password ○ Fingerprint or Password

Boot

It shows windows boot function key using F5/F8 key.

☐ Boot Function Key

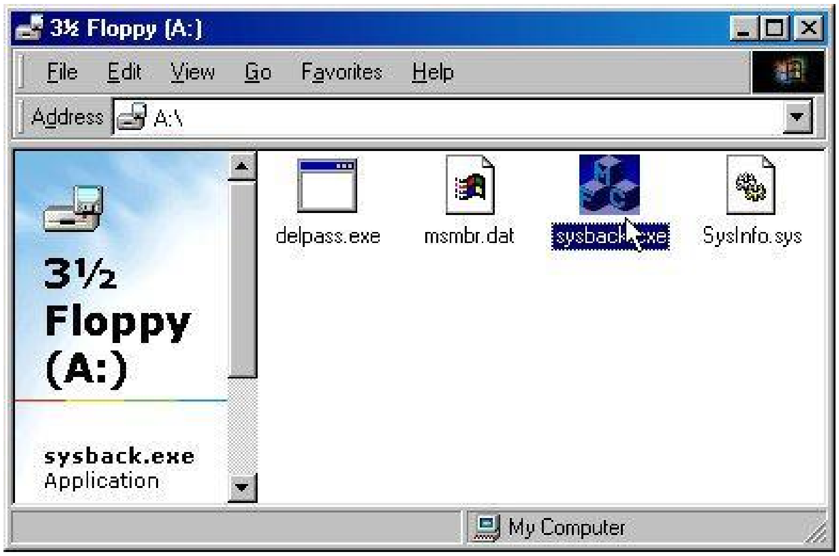
It confirms user with boot protector when booting.

☐ Install Boot Protector

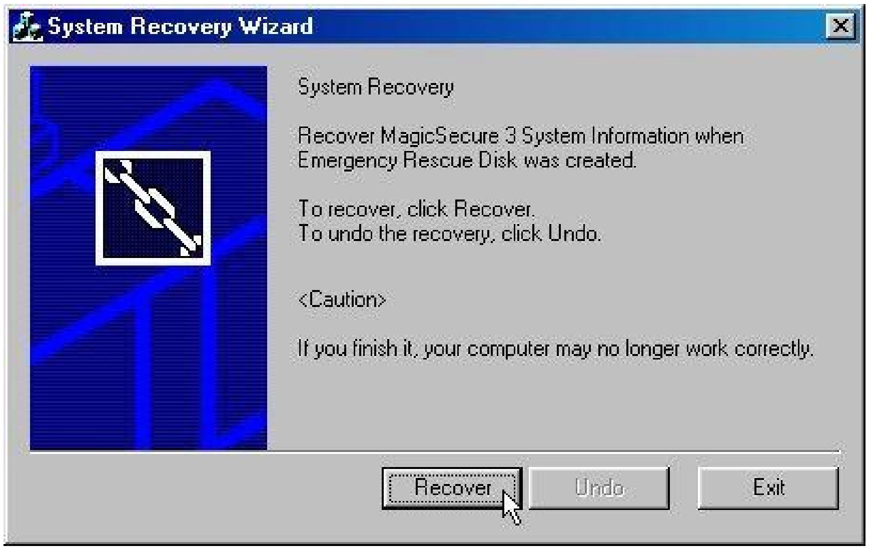
Advanced

Click Encryption Algorithm Settings to select encryption algorithm type, and click Fingerprint Device Settings to modify fingerprint device or see fingerprint image.

Create the Emergency Rescue Disk and modify the system configuration.



In order to recover the system configuration to the point when the Emergency Rescue Disk was created, insert the Emergency Rescue Disk in drive A: and run 'sysback.exe'.



System Recovery

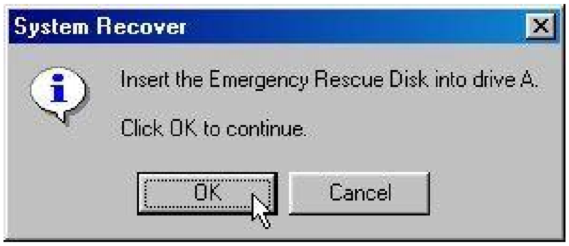
Recover MagicSecure 3 System Information when Emergency Rescue Disk was created.

To recover, click Recover.
To undo the recovery, click Undo.

<Caution>

If you finish it, your computer may no longer work correctly.

The **System Recovery Wizard** window will be displayed. Click **Recover**.

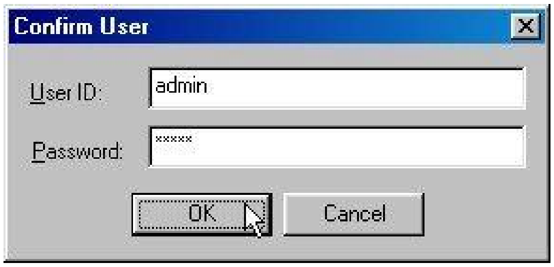


System Recover

Insert the Emergency Rescue Disk into drive A.

Click OK to continue.

Insert the Emergency Rescue Disk into drive A:.

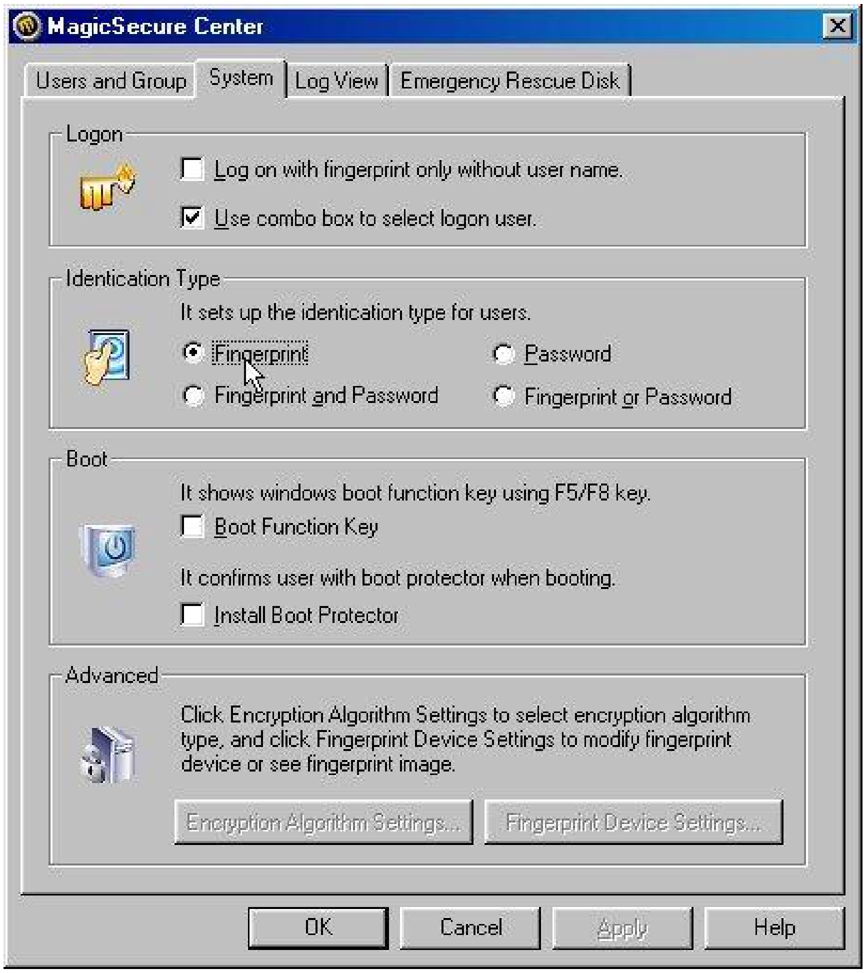


Confirm User

User ID: admin

Password: *****

Input the Emergency Rescue Disk's user ID and password.



MagicSecure Center

Users and Group | System | Log View | Emergency Rescue Disk

Logon

□ Log on with fingerprint only without user name.

☑ Use combo box to select logon user.

Identication Type

It sets up the identication type for users.

● Fingerprint ○ Password

○ Fingerprint and Password ○ Fingerprint or Password

Boot

It shows windows boot function key using F5/F8 key.

□ Boot Function Key

It confirms user with boot protector when booting.

□ Install Boot Protector

Advanced

Click Encryption Algorithm Settings to select encryption algorithm type, and click Fingerprint Device Settings to modify fingerprint device or see fingerprint image.

Encryption Algorithm Settings...
Fingerprint Device Settings...
OK
Cancel
Apply
Help

The figure above displays the recovered system configuration.

2. My SecureDocs

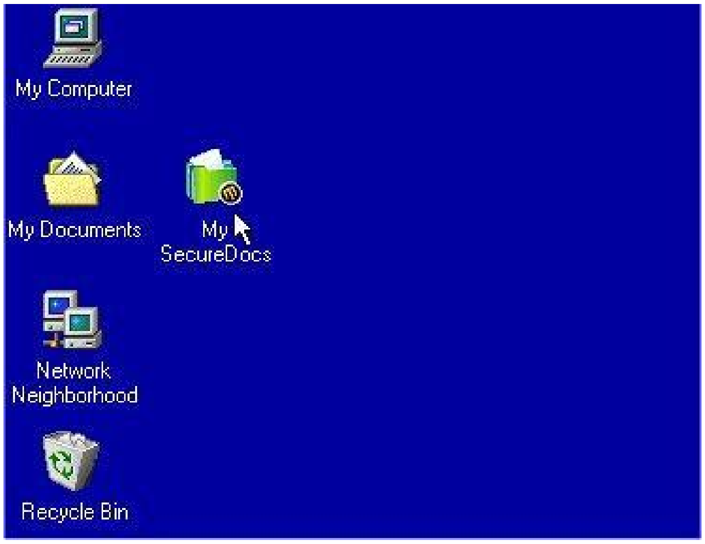
Description

- Just as **My Documents** is used for managing your documents, **My SecureDocs** manages encrypted files and documents.
- There is a folder for each user, and folders encrypted by other users are not seen.
- Each file or folder is displayed with an overlay icon. (A small icon attached to the main icon of the file or folder.)

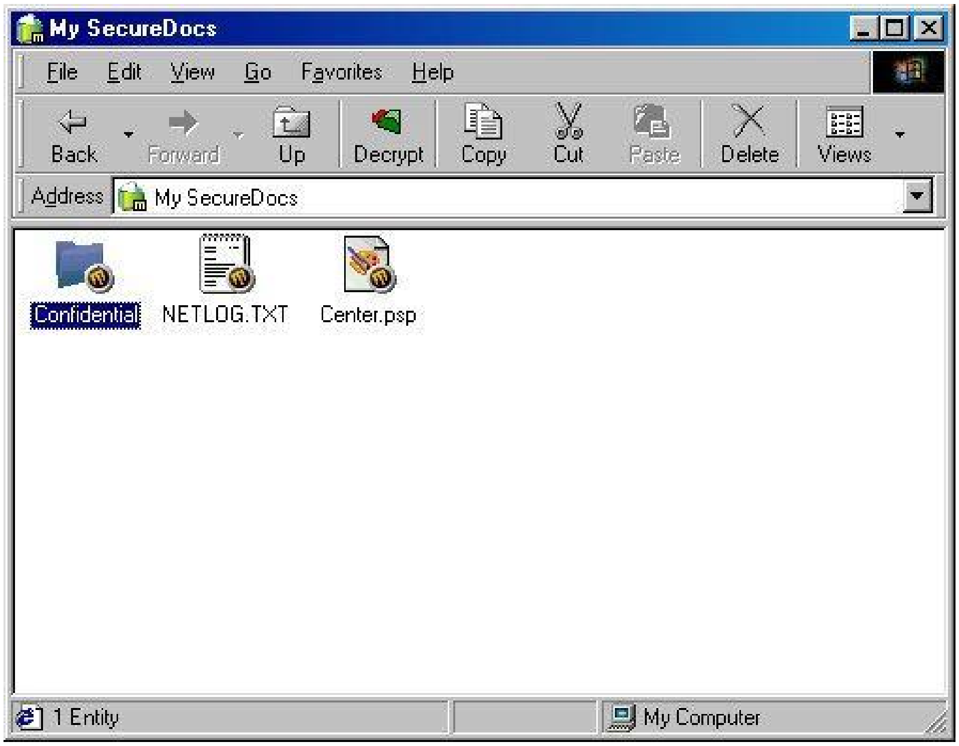
Functions

- **My SecureDocs** provides a toolbar and a context (pop-up) menu to decrypt a file or folder.
- You can move and copy files to/from regular folders using Drag & Drop or Copy & Paste.
- You can view properties of a file or folder.

(1) How to run My SecureDocs

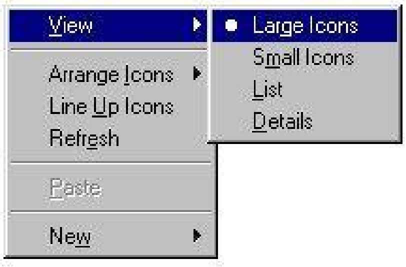


Select **My SecureDocs** from the desktop.



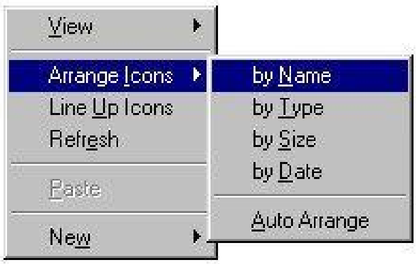
The figure above displays the **My SecureDocs** window.

(2) Viewing icons in My SecureDocs



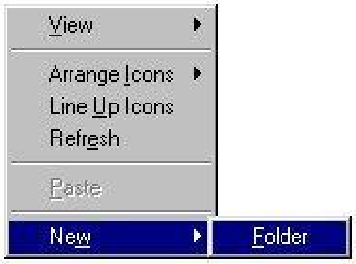
Right-click **My SecureDocs** and select **View**.

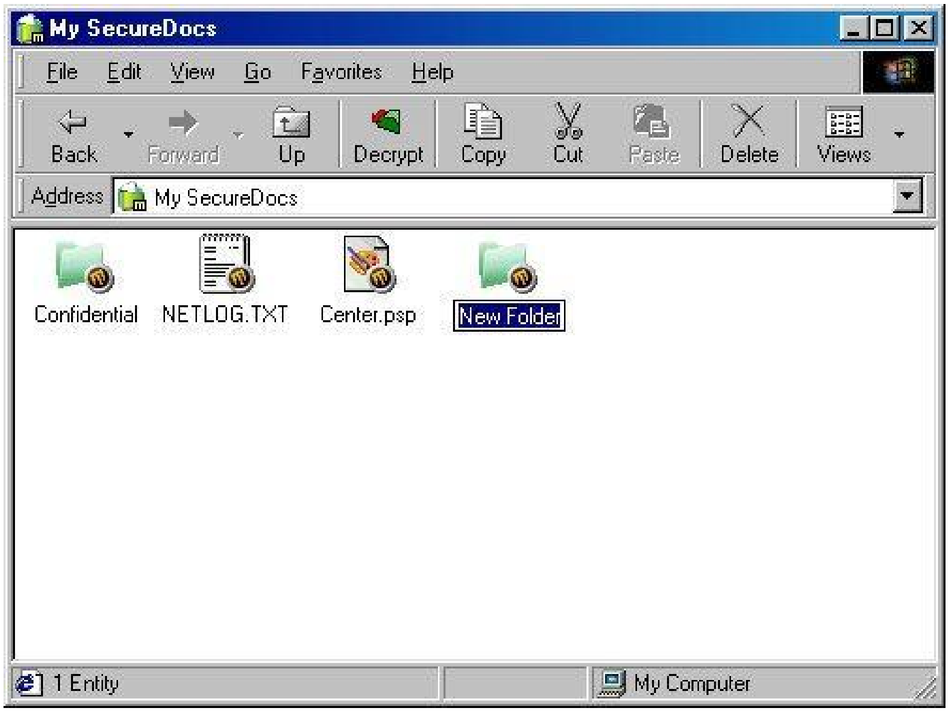
(3) Arranging icons in My SecureDocs



Right-click your mouse from **My SecureDocs** and select **Arrange Icons**.

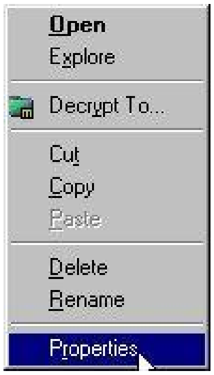
(4) Creating a new folder

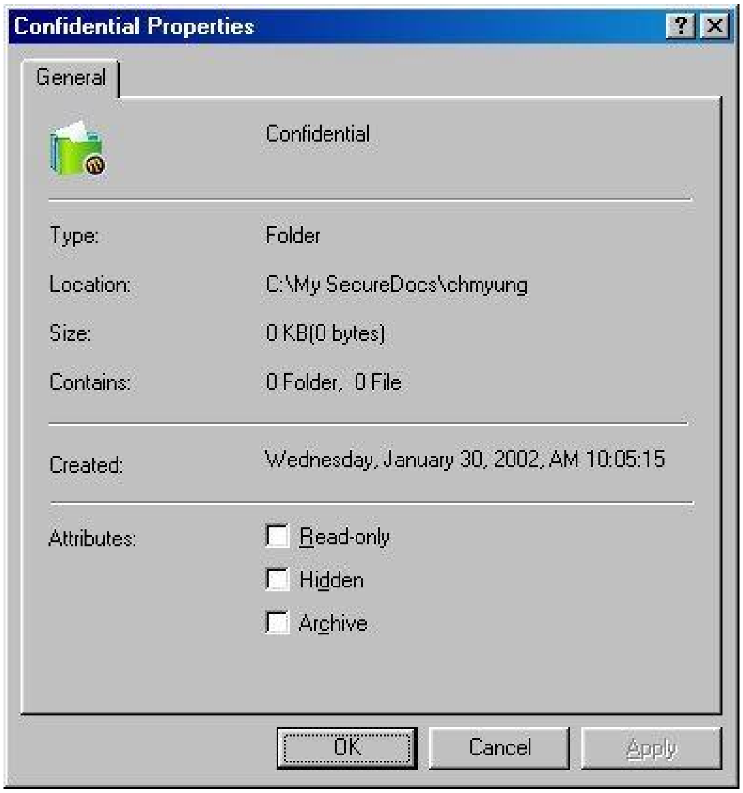




Select **New > Folder** Type in the new folder's name.

(5) Viewing folder properties





Confidential

Type: Folder

Location: C:\My SecureDocs\chmyung

Size: 0 KB(0 bytes)

Contains: 0 Folder, 0 File

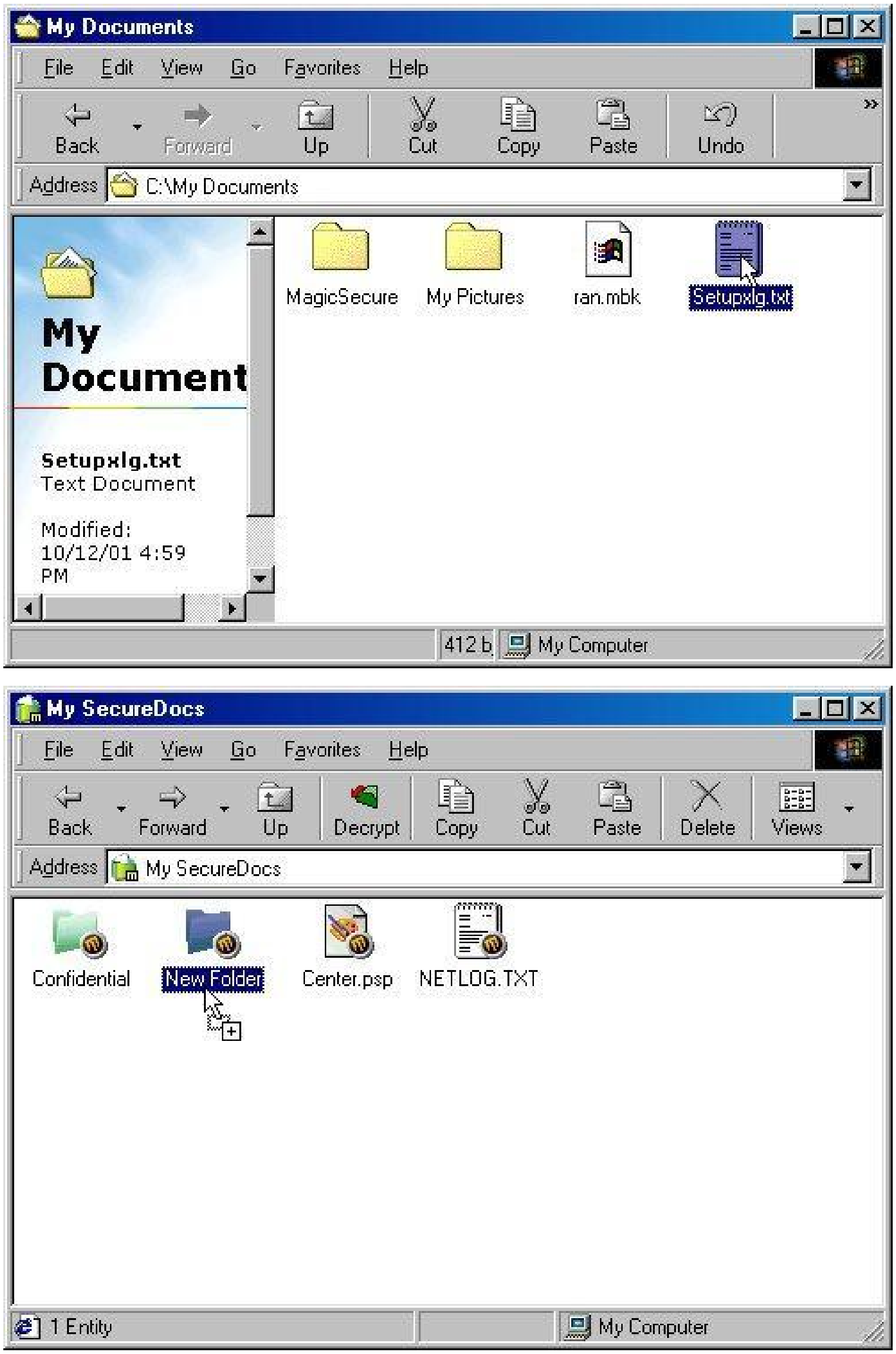
Created: Wednesday, January 30, 2002, AM 10:05:15

Attributes: □ Read-only
□ Hidden
□ Archive

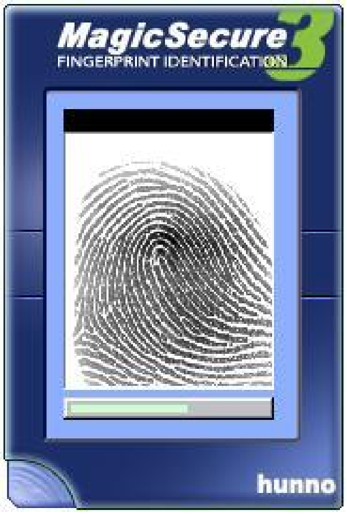
(6) Folder/File Encryption

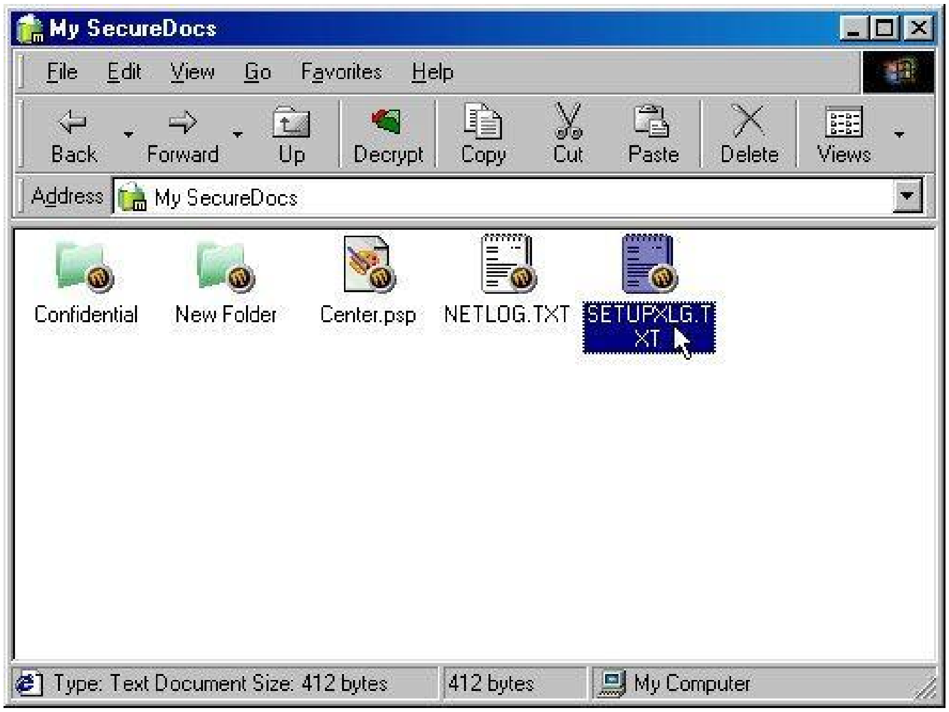
If you move a regular folder/file to **My SecureDocs** using Drag & Drop, **Cut/Paste** buttons on the toolbar, or short-cut keys (^X/^V), the folder/file is automatically encrypted. Folders created in **My SecureDocs** are also encrypted. (Please refer to the **Creating a new folder** section)

Method 1: Moving a document from My Documents to My SecureDocs



The figures above display an example of moving a file (MS3.0_SN.txt) in **My Documents** to **My SecureDocs** using Drag & Drop.

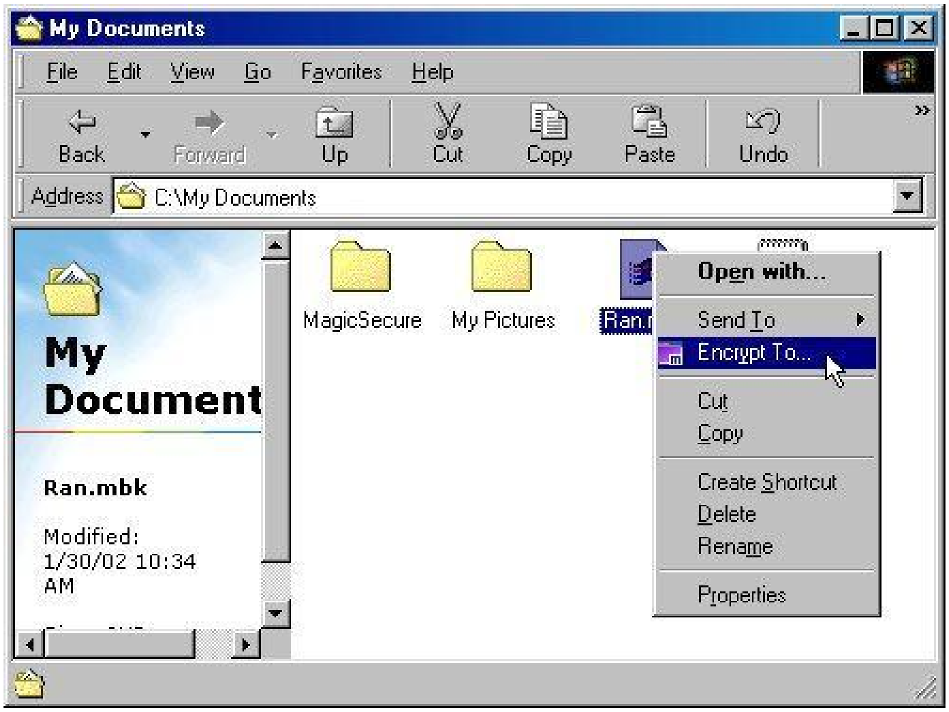




Type: Text Document Size: 412 bytes | 412 bytes

The above figures display the MS3.0_SN.txt file moved to **My SecureDocs** and encrypted after authentication.

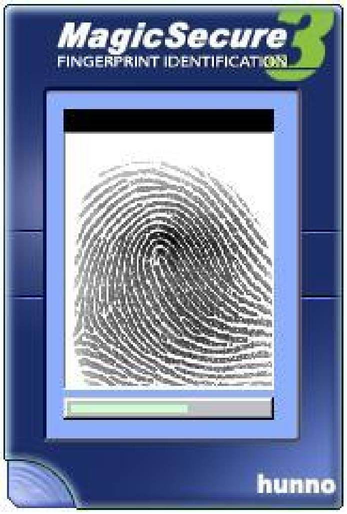
Method 2: Moving a document from My Documents to My SecureDocs



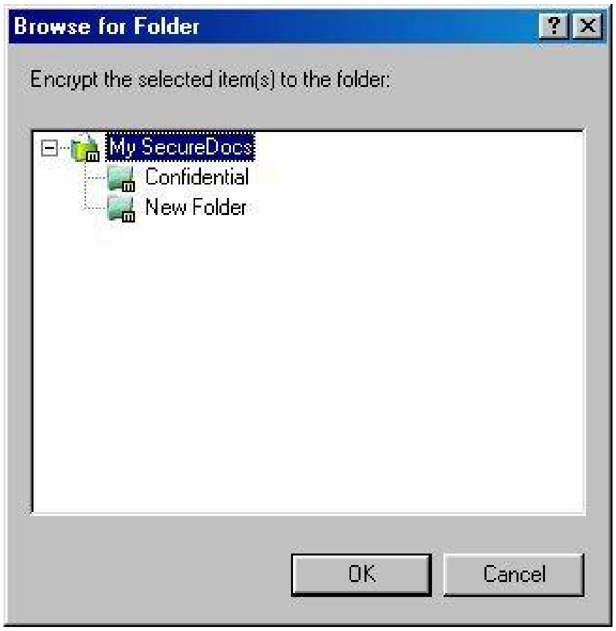
Address: C:\My Documents

Ran.mbk

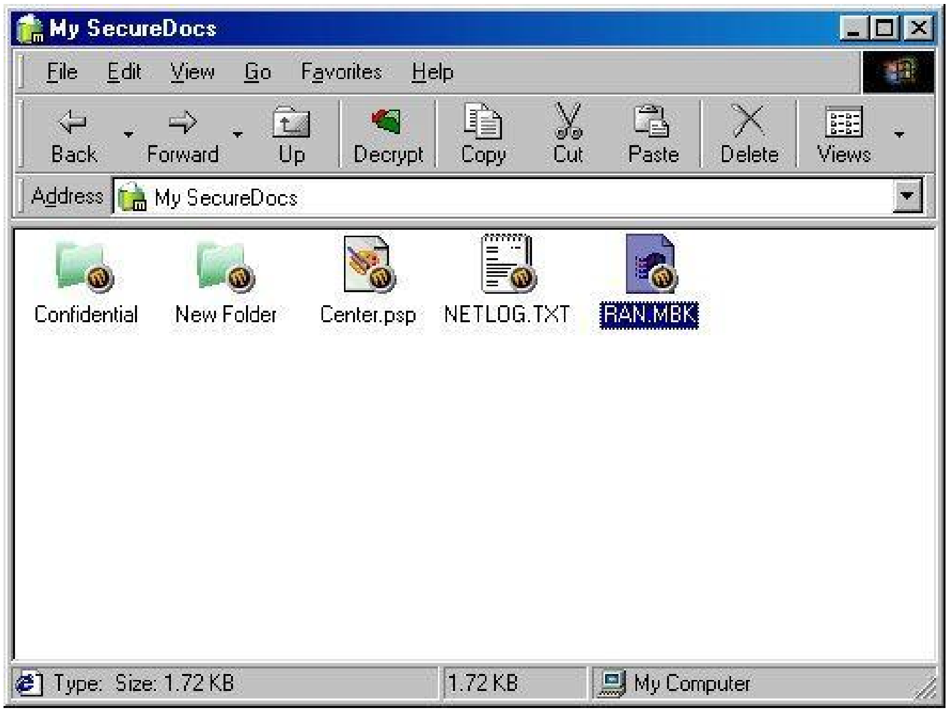
Modified:
1/30/02 10:34
AM



Right-click a file in My Documents and select **Encrypt To…** from the context menu. The Identification window will be displayed prompting you to provide a fingerprint/password.



Encrypt the selected item(s) to the folder:

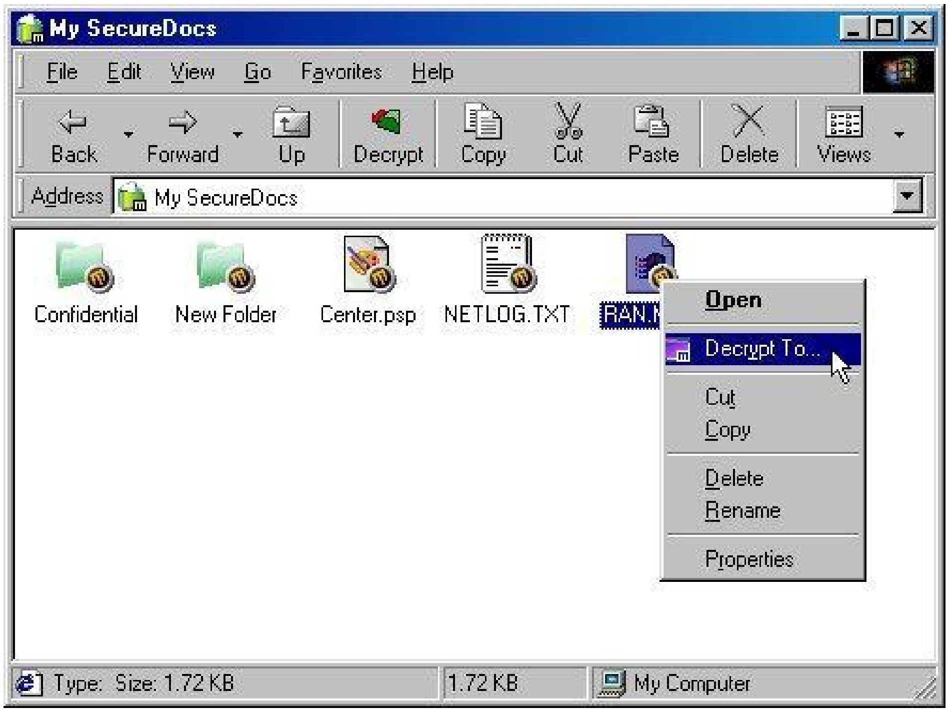


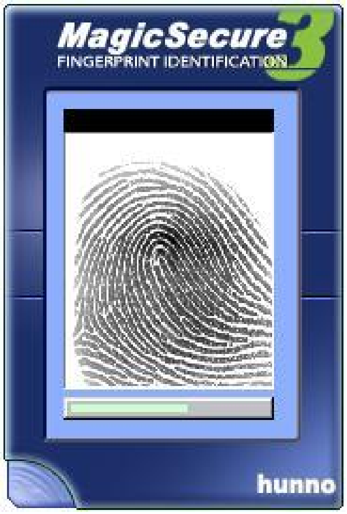
After authentication, select **My SecureDocs** from the **Browse for Folder** dialog box and click **OK**. The file will be added to **My SecureDocs**.

(7) Folder/File Decryption

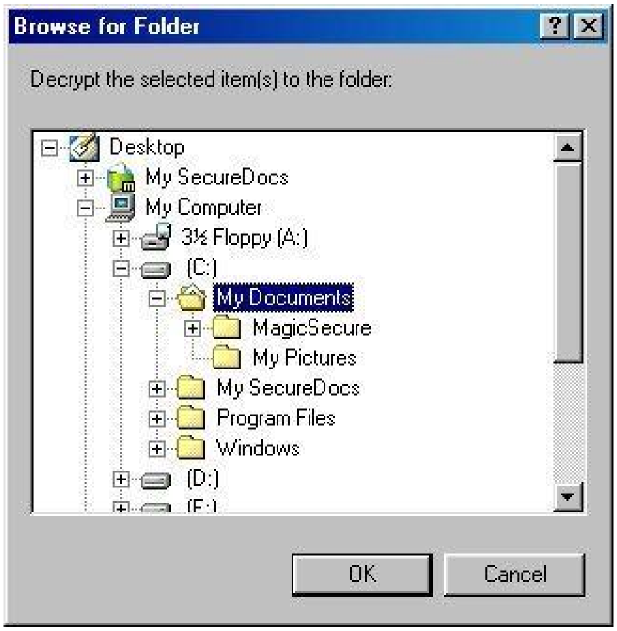
- Since folders and files in **My SecureDocs** are encrypted, they must be decrypted before you copy them to other folders.
- If you move a folder/file out of **My SecureDocs** to a regular folder using Drag & Drop, Cut/Paste buttons on the toolbar, or short-cut keys (^C/^V), the folder/file is automatically decrypted.

① File decryption from My SecureDocs



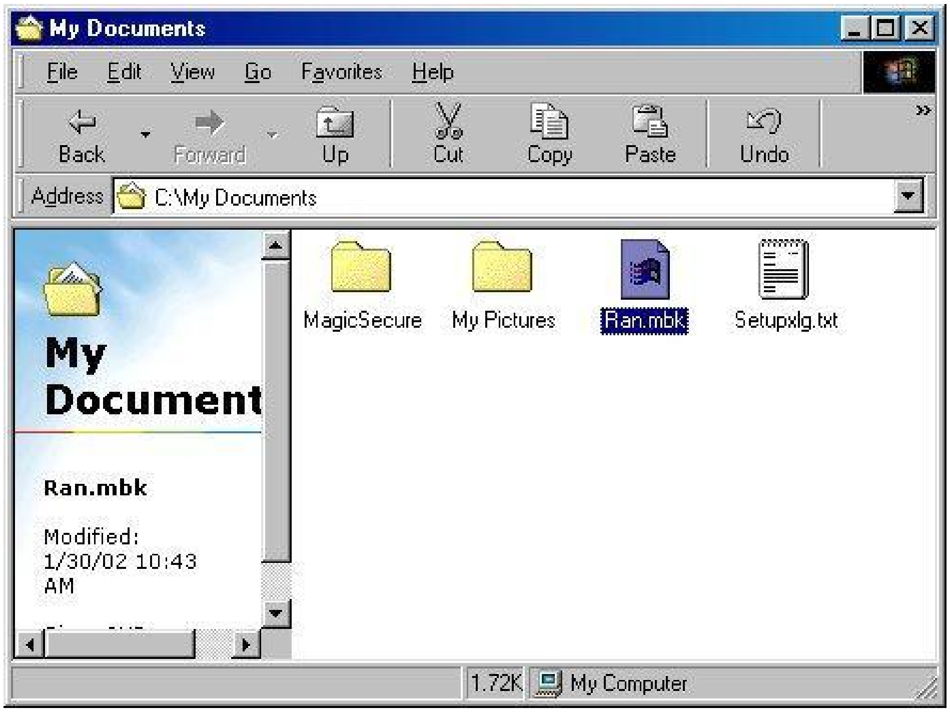


Select an image folder and choose **Decrypt To** from the pop-up menu or click the **Decrypt** button from the toolbar. Complete the Identification procedure.



Browse for Folder

Decrypt the selected item(s) to the folder:



My Documents

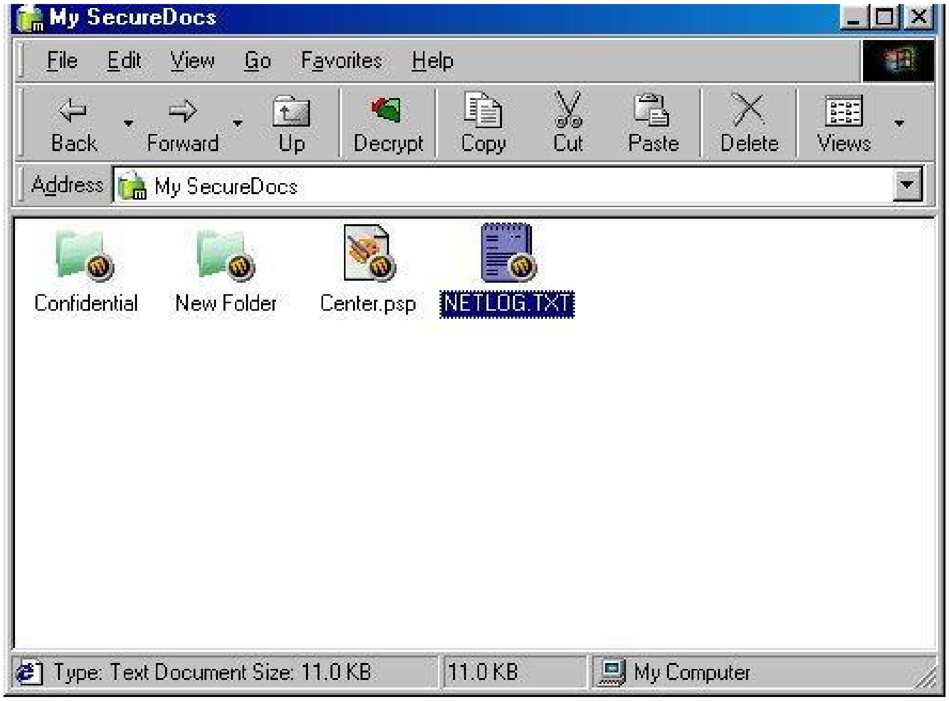
Ran.mbk

Modified:
1/30/02 10:43
AM

1.72K My Computer

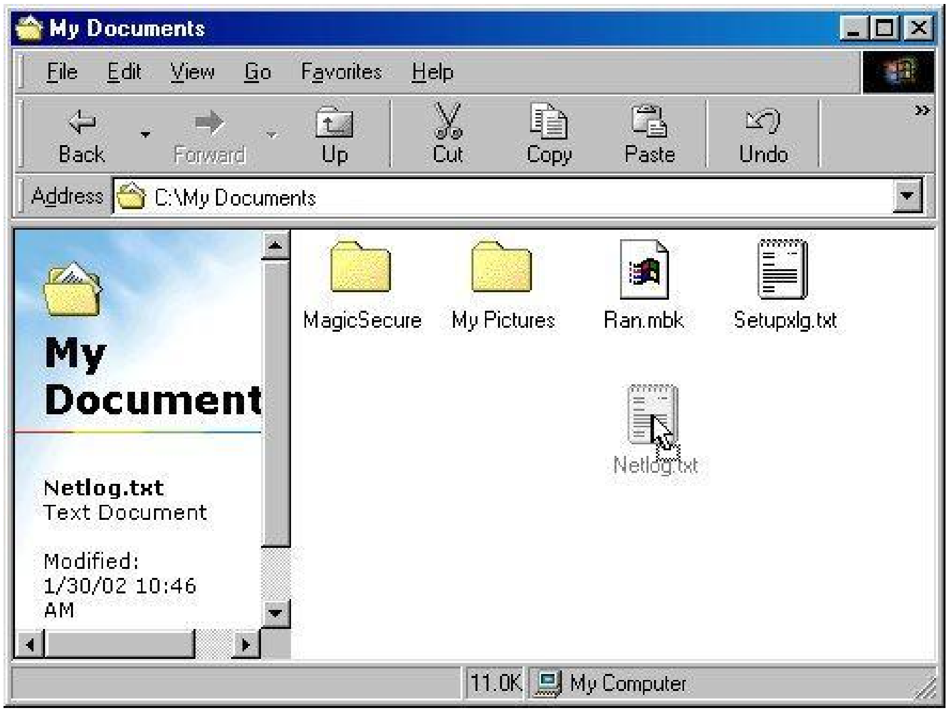
Specify the new location for the file/folder to move to after decryption.

② Decrypting/Moving a file from My SecureDocs to a regular folder



Address: My SecureDocs

Type: Text Document Size: 11.0 KB | 11.0 KB



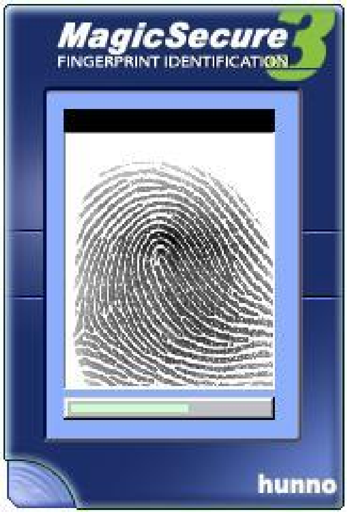
Address: C:\My Documents

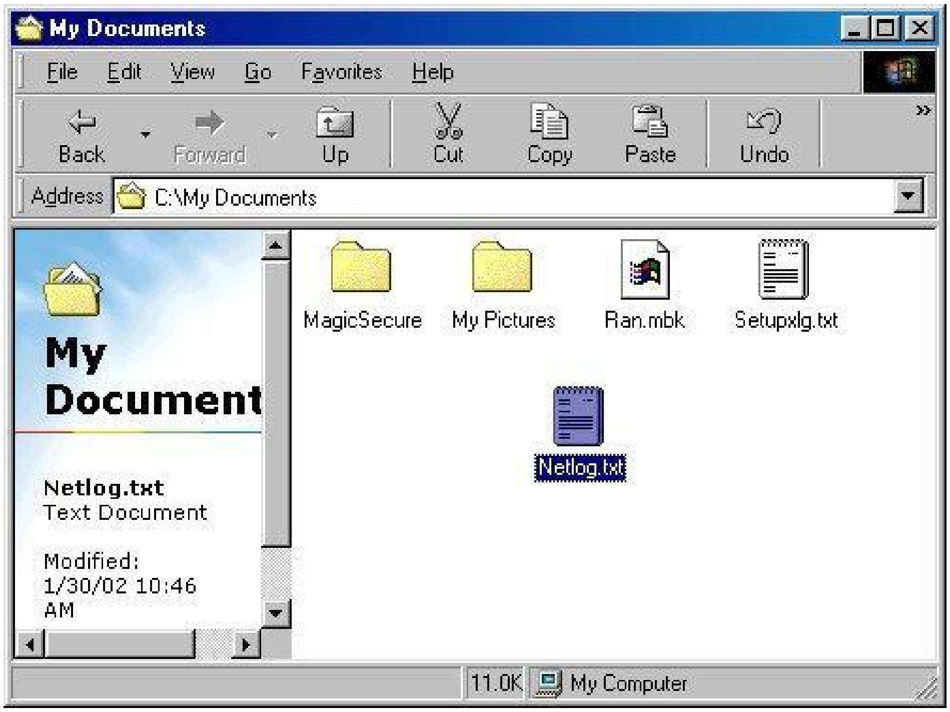
Netlog.txt
Text Document

Modified:
1/30/02 10:46
AM

11.0K

The figures above display a file being moved from **My SecureDocs** to **My Documents** using Drag & Drop.

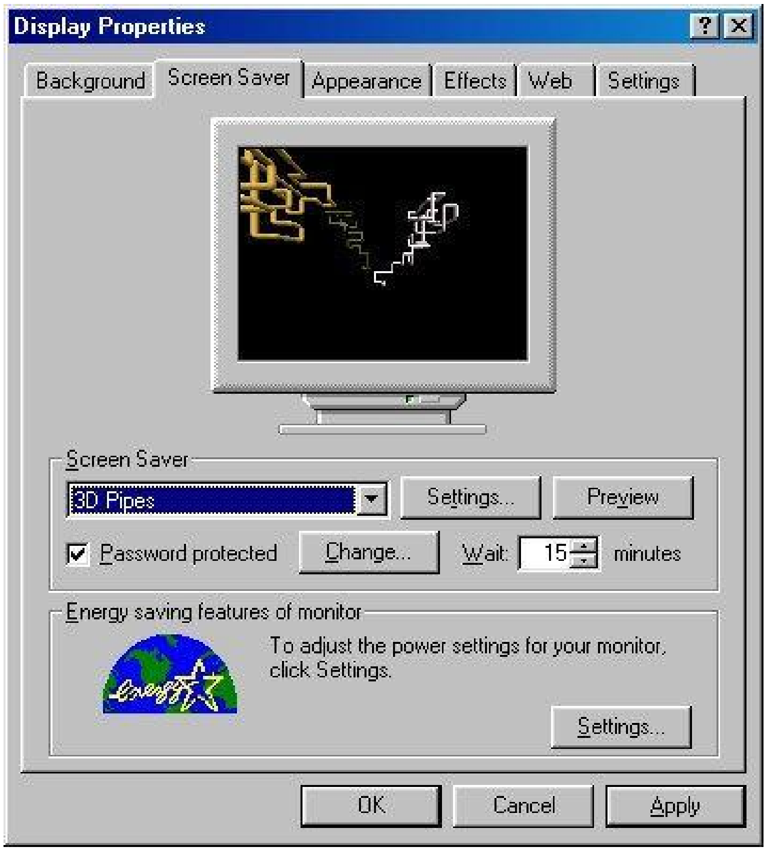




The figure above displays a decrypted file.

3. Screen Saver

Under the Windows environment, when a user leaves his/her computer for a certain period of time, the screen saver is activated to protect the monitor. However, during the user's absence, an unauthorized person may stroke any key to turn off the screen saver and have access to important files and/or documents. In order to prevent this, the system can be configured to request the user for fingerprint/password authentication before turning off the screen saver.



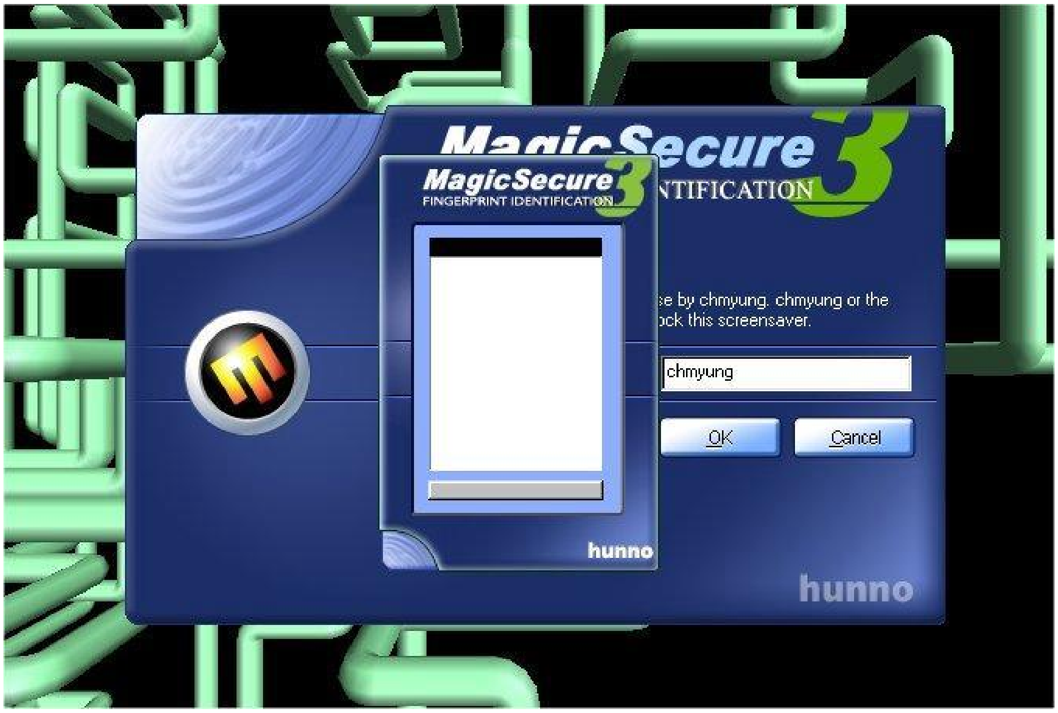
Screen Saver: 3D Pipes

☑ Password protected

Wait: 15 minutes

To adjust the power settings for your monitor, click Settings.

From the **Screen Saver** tab, check the **Password protected** option and click **OK**.



se by chmyung. chmyung or the
ock this screensaver.

chmyung

If the user is absent from his/her computer for a specified amount of time, the screen saver will be activated. Stroking any key while the screen saver is activated will display the fingerprint authentication window. If the fingerprint provided is identical to that of the user, the screen saver will be turned off and the user will be able to return to the work screen.

Chapter 4. Q&A

Q **I am currently using Ramses II ver2.0. How can I upgrade to ver3.0?**

A Ramses II ver3.0 features a new file encryption format to provide enhanced security measures. Therefore, you must completely remove Ramses II ver2.0 before installing version 3.0.

Please note Ramses II ver3.0 cannot decrypt files that have been encrypted with Ramses II ver2.0. You must decrypt all files before removing Ramses II ver2.0 from your system.

※ Ramses I ver1.0 users must take identical steps to upgrade to version 3.0.

Q **I have set the Authentication Method as Password from Ramses II Center's system configuration, but the Fingerprint Authentication window is displayed when I try to encrypt files. Why is that?**

A Each user's properties settings have higher authentication priorities than system configuration settings.

Please check your user properties and verify whether the authentication method is set to 'Fingerprint'.

Q **I have encrypted and saved documents (Hangul or MS Word) in My SecureDocs. Can I open documents saved in My SecureDocs using corresponding application programs?**

A In order to facilitate working with documents, Ramses II ver3.0 allows users to open/edit/save documents in 'My SecureDocs' using corresponding application programs.

Q **I have installed and used Ramses II without any problem. However, all of a sudden, I can't register or authenticate fingerprints.**

A Wipe the fingerprint recognition sensor with a clean cloth and try again. If the problem persists, please contact our customer service department.

Q **When I try to change the system configuration to set the Authentication Method to Fingerprint, a message is displayed indicating that 'There is a user without a fingerprint registered. Cannot change Authentication Method.'**

A The message implies that the user who installed the program (the initial administrator) did not register a fingerprint. Once the program installer (the initial administrator) registers his/her fingerprint, the message will not be displayed when changing the authentication method.

Q **The authentication method is set to Password, but I have forgotten my password and cannot log on.**

A You must have the Emergency Rescue Disk. Insert the disk when the authentication screen is displayed to log on to your computer.

Q **What is the maximum number of users that can be registered?**

A There is no limit in the number of registered users.

Q **What is the administrator's security level setting?**

A It indicates the Fingerprint Authentication Level. Increasing the security level will declare authentication successful only when there is a very high degree of a fingerprint match.

Try decreasing the Security Level if your fingerprint is not vivid or requires repeated registration attempts.

Q **What operating systems are compatible with Ramses II?**

A Ramses II is compatible with Windows 98/98SE/ME.

Q **I have connected the fingerprint recognition sensor to my computer, but the Hardware Installation Wizard does not run.**

A Check your CMOS settings and verify whether the USB port is enabled.

If the Plug & Play feature does not function properly, even after enabling the USB port, please contact our Customer Service.

Software License Certificate

Product Name: Ramses II® ver3.0 Standard Edition
Serial Number:

The user license is granted regarding this software product, including the program, documentation and recording medium, to the user or group entitled to the serial number above.

This software product is protected under Korean and international copyright laws, including the Computer Program Protection Law.
Any aspect of usage of this software product must comply with the Software License Agreement.

This Software License Certificate is proof that you have purchased the product. Since it is required for receiving upgrades or services, please keep it in a secure place.

Ramses II ver3.0 Software License Agreement

This agreement is a legal usage license agreement between Immanuel Electronics co., ltd. and the user, and not an agreement of transaction.

By unpacking the CD-ROM package, you agree to be bound by the terms of this agreement.

If you do not agree with the terms of the agreement, please return the product promptly.

If you return the product, you will receive a refund.

1. Usage License

Immanuel Electronics co., ltd., grants you the license to use this software as indicated in the User Certificate.

The software is considered 'being used' if it is stored in a computer's main or other storage device. The number of software copies will be determined by taking the greater number of the number of computers 'used' by the software and the number of computers with the software stored.

2. Right to Upgrade

If you have purchased the software by upgrading an older version, the usage license of the old version is transferred to the new version. However, you may only use the old version under the condition that the old and new versions are not running simultaneously. Therefore, you are prohibited from transferring, renting or selling the old version. You maintain the usage license for the program and ancillary files that are in the old version but not in the new version.

3. Assignment of License

If you wish to transfer the usage license of this software to a third party, you must first obtain a written statement indicating that the recipient agrees with this agreement. You must then transfer the original disk and all other program components, and all copies of the program must be destroyed. After the transfer is complete, you must notify Immanuel Electronics co., ltd., to update the customer registration.

4. Copyright

All copyrights and intellectual properties of the software and its components belong to Immanuel Electronics co., ltd., and these rights are protected under Korean and international copyright laws. Therefore, you may not make copies of the software other than for your backup purposes. In addition, you may not modify the software other than for reverse-engineering purposes to secure compatibility. Finally, you may not modify, transform or copy any part of the documentation without written permission from Immanuel Electronics co., ltd., (If you're using a network product, you may copy the documentation in the amount of the number of users)

5. Installation

An individual user can install this software in his/her PCs at home and office, as well as in a mobile PC. However, the software must not be running from two computers simultaneously. A single product can be installed in two or more computers in one location, but one of those computers must have a usage rate of at least 70%. If another computer has a usage rate of 31% or higher, another copy of the software must be purchased.

6. Limitation of Warranty

Immanuel Electronics co., ltd., guarantees that the CD-ROM and all components are free of physical damage for the 90 days after purchase. If you find any manufacture defect within the warranty period, we will replace the product. You must be able to prove that the product has been purchased within 90 days to receive a replacement, but we will not replace a product damaged due to your mishandling or negligence. Immanuel Electronics co., ltd., does not guarantee that the software and its features will satisfy your specific needs, and is not liable for any consequential damages arising out of the use of this product.

7. Liabilities

Immanuel Electronics co., ltd., is not liable for any verbal, written or other agreements made by third parties, including product suppliers and dealers.

8. Termination

This agreement is valid until the date of termination. However, the agreement shall terminate automatically if you damage the program or its components, or fail to comply with the terms described in this agreement.

9. Policy on Registration and Change

In order to receive customer services and revised versions, individual and group users must fill out the attached Customer Registration Card and send it to Immanuel Electronics co., ltd., Immanuel Electronics co., ltd., provides customer services only to registered users. Furthermore, registered users will be able to receive later versions at discounted prices.

10. Customer Service

Immanuel Electronics co., ltd., makes every effort to provide registered customers with technical assistance and solutions to problems regarding software applications under certain system environments. When a customer submits a suggestion about any inconvenience or anomaly experienced during product usage, Immanuel Electronics co., ltd., will take corrective action and notify the customer of the result.

11. Acknowledgement

You acknowledge that you have read, understood and agree with the terms of this agreement. You also recognize the fact that this agreement has precedence over user agreements of older versions, past order agreements, advertisement notifications and/or other written agreements.

12. Contact

If you have any questions about this agreement, please contact Immanuel Electronics co., ltd., via telephone, fax or e-mail.