

PC E-Lock Smart Commercial V9.0

User Manual



Copyright(C) 2003-2007 Returnstar Electronic Information Co., Ltd.

Web: <http://www.recoverystar.com>

Tel: +86-591-83385086, 87274373

Fax: +86-591-87274383

E-mail: master@recoverystar.com

Important Statements:

1. Use this product strictly according to detailed operation instruction in this User Manual so as to ensure proper use. Please read the instruction thoroughly to save the installation time.

2. If this product is defective, please return it to the appointed agent or our company, together with your original sales receipt or invoice for replacement.

3. Returnstar Electronic Information Co., Ltd. is not liable for any consequential, incidental or indirect damages (including damages for indirect personal injury, loss of business profits, business interruption, loss of business information and the like) arising out of the use or inability to use this product.

4. The product includes enclosed software, later issue and update as well as correlative electronic documents and printing material. By installing, copying, downloading, visiting or using this product in any way, you agree to the terms and conditions of all the clauses in this user manual. The agreement on these clauses has the same effect as one signed through formal negotiation. You may not use this product unless you have agreed to all the clauses in this user manual

5. Returnstar Electronic Information Co., Ltd. will not accept returns of opened packages.

6. Special Notice:

- Please do not deliberately attack or use other tool software to destroy the product's normal running, or run FDISK/MBR, repartitioning, or low formatting after boot from FD or CD. Otherwise this company assumes no liability for all losses arising herefrom, express or implied.

- Please do not apply in the important occasions such the important network service as the satellite launch, the missile guide, the military control, the national secret, etc, without authorization of Returnstar Electronic Information Co., Ltd. Otherwise this company assumes no liability for all losses arising herefrom, express or implied.

- Regular backup of important data is still necessary when using this product. Returnstar Electronic Information Co., Ltd. does not undertake any compensation responsibility for any losses of HD arising from insufficient backup.

Copyright

Your purchasing of this product does not mean that Returnstar Electronic Information Co., Ltd. has transferred the Intellectual Property Right. The product (includes but not limited to any trademarks, images, photos, flash, video, recording music, writing and additional procedure, and other relative product), enclosed printed material, and any copies made in authorization of Returnstar Electronic Information Co., Ltd. are products of Returnstar Electronic Information Co., Ltd. and their Intellectual Property are owned by Returnstar Electronic Information Co., Ltd. The name of the product and all its copies are consistent in CD and the manual. The framework, organization and source code of this product are Returnstar's valuable commercial secret and may not be transferred. This product is protected by PRC Copyright Law, related international treaties, the laws in the product using country.

No part of the product may be copied, modified, rented, leased, transferred in any ways without the writing permission or authorization of Returnstar Electronic Information Co., Ltd., You are allowed to use one product on one computer only. Any reverses engineering, decompiling, and decoding of this product, and retrieving the source code of the product by other ways is also prohibited.

Returnstar, Returnstar Jindun, Recoverystar, and PC E-Lock are registered trademarks of Returnstar Electronic Information Co., Ltd. Any modification of Copyright marks, product names and brand names of this product and its copies is strictly prohibited.

Returnstar Electronic Information Co., Ltd. reserves all rights to charge the fee at anytime for product replacement, revision and update. The information in this document is subject to change at anytime without notice.

Chapter 1 Product Introduction

Returnstar PC E-Lock software is one suite of behavior control and security management product, which is researched and developed by Returnstar Electronic Information Co., Ltd for years of endeavor. It has the following 5 versions:

1. Family Flagship Version: This version is suitable for parent who is not good at computer to control their children's computer behavior at home.

2. Family Perfect Version: This version is suitable for administrator (parent) to control their children's computer behavior at home.

3. Finance Version: This version is suitable for financial personnel or common users. It is an effective tool in computer behavior control and security management.

4. Commercial Version: This version is suitable for businessmen and other users who have requirements in computer behavior control and security management.

5. Full Capability Version: It integrates all functions of Family Perfect Version and Commercial Version. It is suitable for other consumer group to use in different environments and management habit, and guarantees the effective management of the same computer in different environments.

Returnstar Electronic Information Co., Ltd has become a global leader in the computer behavior control and security management. It is the only one solution provider of the comprehensive and perfect computer behavior control and security management for family, commerce, enterprise, office, internet cafes, school computer lab, factory, network center. These solutions (including PC E-Lock, HDD Lock, Personal Key, Net work Alarm System and Network Monitoring System) greatly enhance the efficiency of computer behavior control and security management for computer user and administrator, and solve the key problems on computer management which had disturbed PC users all over the world.

This is an installing and operating manual for Returnstar PC E-lock Smart Commercial.

Chapter 2 Product Characters

Returnstar PC E-lock Smart Commercial version has the following strong features:

2.1 Easy to install and use. Anyone who knows a little about the computer can acquire the operation in 10 minutes.

2.2 Support Windows 2000/XP/2003, it is compatible with all hardware and software when installing and using

2.3 Resist deleting, tracking by special program, uninstalling and modifying the catalogue, file, and the program of the product after it is installed. So you do not need to worry about that someone will rename, modify, delete, uninstall or dismiss the product.

2.4 Resist deleting the program and terminating its running through registry or task manager while running the product. So you do not need to worry about termination of the running by other people.

2.5 Function validly under Windows OS safe mode.

Chapter 3 Product Install Register and Uninstall

3.1 System Requirements:

Ensure your PC has the following characters:

- 80X 86 compatible computer systems
- More than 500 MB HDD free space, and more than 32MB memory.
- Operating System: Windows 2000/XP/2003.
- Make sure you have installed LAN Card in the computer.

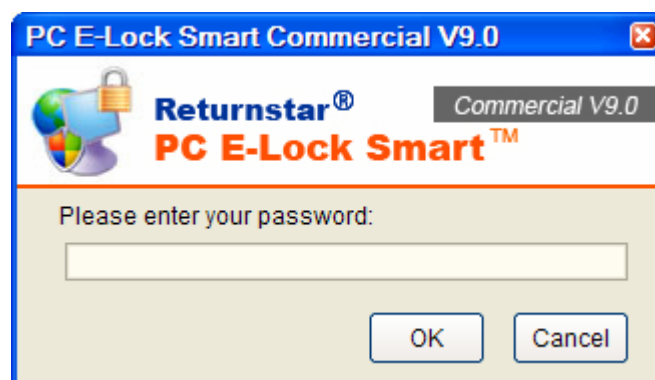
3.2 Product Install



Important Statement: *The product series has been significantly upgraded. If your version is under V9.0, uninstall it after decrypting the files (folders) and secret disk and then install the new version V9.0.*

Click “*SETUP.EXE*” to install the product, and then finish it according to the prompt.

After installing, please restart the computer and enter the OS. Press “**CTRL+SHIFT+C**” to popup Product Login window, please refer as follows:



On the Login Window, click “*OK*” directly to enter the Product Main Interface (the primary password of administrator is blank, so you do not need to enter

it),.As follows,



Prompt: As the primary password of administrator is blank, please set your password in time.



3.3 Uninstall

Under the login state, click “*SETUP.EXE*” to uninstall and then finish it according to the prompt on Uninstall Interface. Please make sure to restart computer after uninstall.



Caution: Because of the speciality of the product, any shortcut will not be created either on program menu and desktop in OS, or on [add and remove program] after setup.

Chapter 4 Product Usage

4.1 Work Mode

This product has two working modes: Administrator Mode and Controlled Mode.

Administrator Mode: The computer can be used without any limitation in this mode, namely it is under an uncontrolled mode. You can set functions of the PC E-Lock software under the Administrator mode.



Caution: "Data Security" and "My Log" can only work under Administrator Mode.

Controlled Mode: The product will control the computer and limit the system utilization according to your set parameter in this mode. Namely it is under Controlled Mode.

Switch Working Modes: Two work modes can be freely switched by Login and Logout.

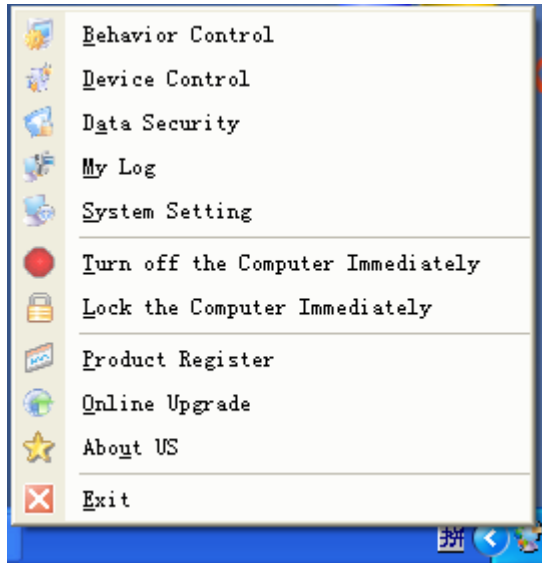


Prompt: when your PC E-lock Smart unregistered is used out of 30 times, it will automatically switch to the Administrator Mode.

4.2 Product Login

Press "**CTRL+SHIFT+C**", it will automatically popup the Login Window. Input the administrator password in the window, and click "OK" to directly enter into the Main Interface, or display small icon in the taskbar at the lower-right corner of the desktop. After successful login, click the small icon in the taskbar to enter into Main Interface, or right-click the small icon to display the following shortcut menu,



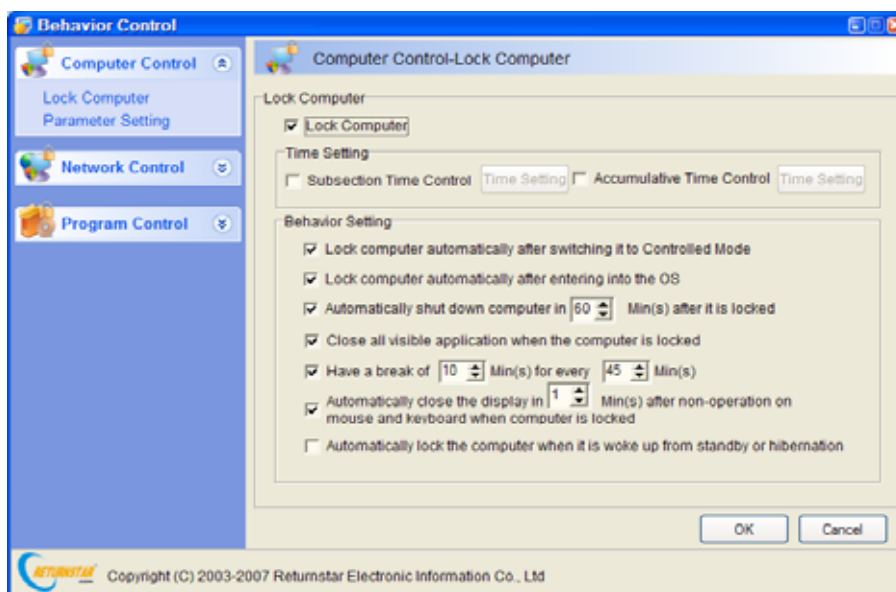


4.3 Behavior Control

Provide functions of “*Lock Computer*”, “*Network Control*” and “*Program Control*”. Effectively control PC start, and the use of network and software under Controlled Mode.

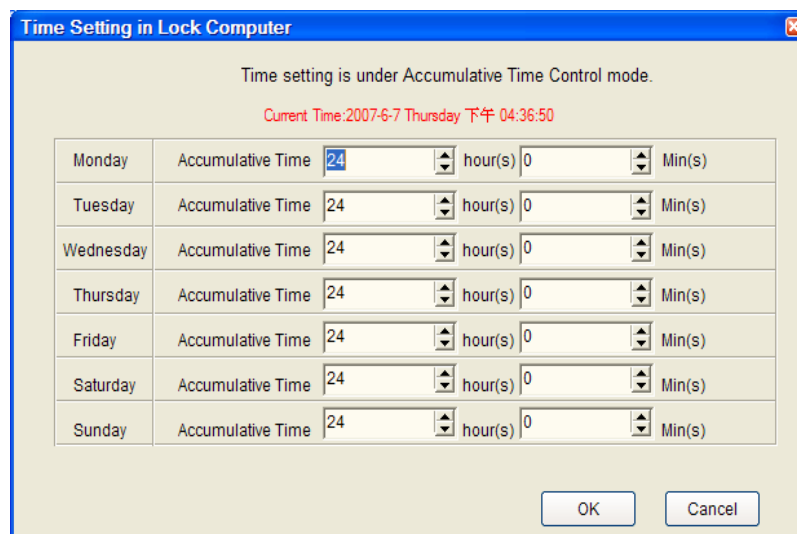
4.3.1 Lock Computer

Provide functions of “*Time Setting*”, “*Behavior setting*”, and “*Parameter Setting*”. You can conduct time setting in “*Lock Computer*” and regulate the behavior when or after locking computer; it is convenient for user to manage the computer. Please refer as follows:



4.3.1.1 Time Setting

Control the computer according to your Subsection and Accumulative Time Control setting here. The system default is “Unlock” all time, and the default Accumulative Time is 24 hours per day.



Prompt: If the Subsection Time Control and Accumulative Time Control are set simultaneously, both of them will work. The rule is obeyed in the settings referred to the Subsection Time Control and Accumulative Time Control.

4.3.1.2 Behavior Setting

Set the conditions of automatically locking the computer and the computer activities when or after it is locked. It is a very important measure for Behavior

Control.

Lock the computer automatically after switching it to the Controlled Mode:

Once the function is selected, it will lock the computer automatically any time you switched to Controlled Mode. The system default is “*enabled*”.

Lock the computer automatically after entering into the OS: Once the function is selected, it will automatically lock the computer after entering OS. The system default is “*Enabled*”.

Automatically shut down computer in [] minutes after it is locked: Once the function is selected, computer will automatically turn into PC E-Lock Screensaver after being locked at any time or in any way, and be shut down in 0-60 minutes. The system default is 60 minutes and “*Enabled*”.

Close all visible applications when the computer is locked: When the computer is locked, all open applications in the taskbar will be closed. The system default is “*Enabled*”.

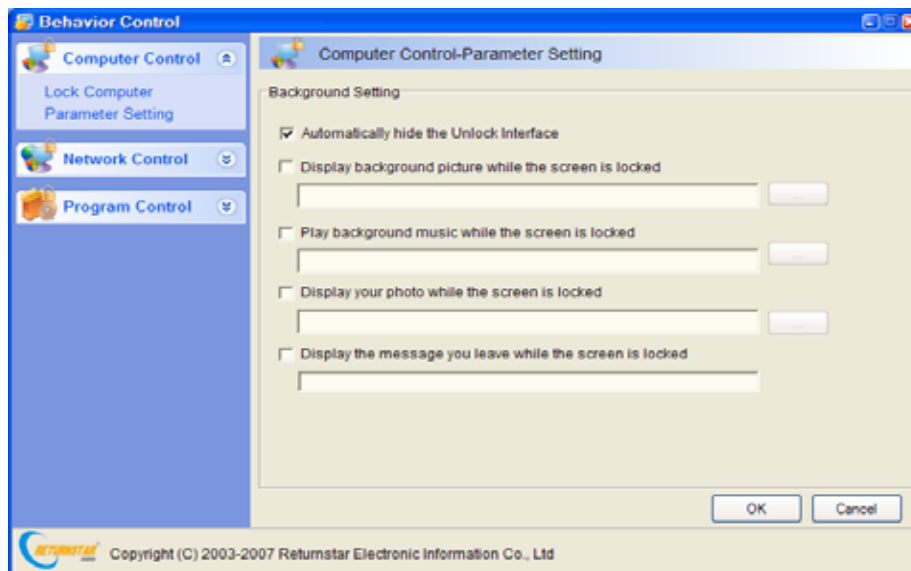
Have a break of [] Min(s) for every [] Min(s): To protect eyesight and adjust the sitting posture, 1-30 minutes break will be made for users when computer has been used for every 1-90 minutes. The system default is “*Have a break for 10 minutes for every 45 minutes*”. Once the using time ends, it will automatically turn into the PC E-Lock Screensaver. At that time, if someone forces to shut down the computer, it will automatically turn to the PC E-Lock Screensaver mode after being restarted. When the break time is over, the computer will return to the available state automatically. The system default is “*Enabled*”.

Automatically close the display in [] minutes after non-operation on mouse and keyboard when computer is locked: When the computer is locked, it will automatically close the display in 1-60 minutes after non-operation on mouse and keyboard in order to protect the display. User who would like to use the computer just needs to move the mouse slightly or press the keyboard, system will automatically turn to PC E-Lock Screensaver. The system default is “*Enabled*” and “*one minute*”.

Automatically lock the computer when it is woke up from stand by or hibernation: At that time, if someone forces to shut down the PC, it will automatically turn to the PC E-Lock Screensaver mode after being restarted. The system default is “*Disabled*”

4.3.1.3 Parameter Setting

Set the Background characters of PC E-Lock Screensaver which appears when the computer is locked, such as “*Play background music*”, “*Display administrator’s photo and message information*”, etc. Please refer as follows,



Automatically hide the Unlock Interface: After locking computer, the system will automatically turn into the PC E-Lock Screensaver. The Unlock Dialog Box will be automatically hidden. Move mouse slightly or press the keyboard, the system will automatically display the Dialog Box when user would like to unlock and use the computer. The system default is “*Enabled*”.

Display the background picture while the screen is locked: Set your background picture as the PC E-Lock Screensaver Interface. To avoid pattern distortion, users had better to choose the picture size according to your display resolution. We provide some delicate background patterns for download in our website, including 1024x768 and 800x600 image size. The system default is “*Disabled*”.

Play the background music while the screen is locked: When computer is locked, the system will play your set background music circularly with the PC E-Lock Screensaver Interface appeared. It can support *.mid、*.wma、*.mp3 files. We provide some euphonic background music for download in our website. The system default is “*Disabled*”.

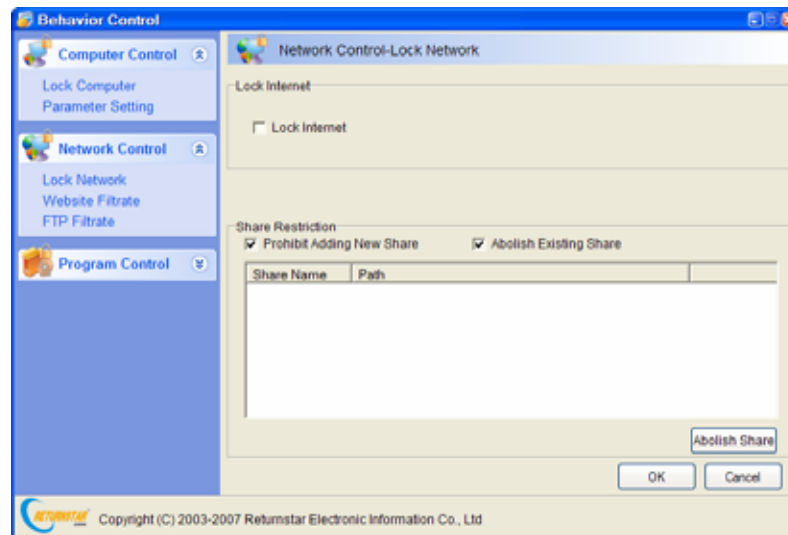
Display your photo while the screen is locked: Displays your photo on the PC E-Lock Screensaver Interface. The photo size is of 80 X 70 pixels. The system default is “*Disabled*”.

Display the message you leave while the screen is locked: Display the

rolling message you leave on the PC E-Lock Screensaver Interface. The system default is “Disabled”.

4.3.2 Network Control

Provide functions of “Lock Network”, “Filtrate Website” and “Filtrate FTP”. Effectively control the using of network under Controlled Mode. Please refer as follows,



4.3.2.1 Lock Network

Provide functions of “Lock Internet” and “Share Restriction”. On the “Lock Internet”, the system default is “Disabled”.



Prompt: After you have selected “Lock Internet”, please restart the computer. Then PC E-Lock will lock all functions related to network automatically. The chatting tools and other programs relative with internet will fail in connecting with internet.

Provide “Prohibit Adding New Share” and “Abolish Existing Share” functions on the “Share Limitation”. Click “Prohibit Adding New Share” to forbid adding new share under Controlled Mode. Contrarily, unclick it to permit adding. The system default is “Enabled”. Click “Abolish Existing Share” to abolish the current existing share from the share list. Firstly select the share item from list, and then click “Abolish Share” button. The “Abolish Existing Share” function is efficient directly under Administrator Mode. The function we designed is for users to directly operate all system shares and avoid possible forgetting because of too much shares effectively.

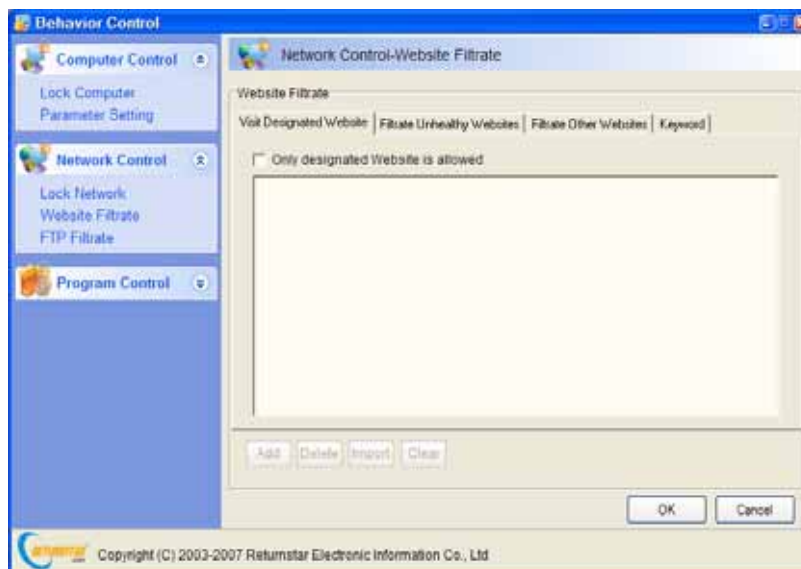
4.3.2 Website Filtrate

Provide functions of “Visit Designated Website”, “Filtrate Unhealthy Website”, “Filtrate other websites”, and “Filtrate Keyword”. Through website filtration, you can effectively control your visiting websites. Under Controlled Mode, if you select “Visit Designated Website” only the websites from designated website list can be visited; select “Filtrate Unhealthy Website” and “Filtrate Other Websites”, the system default is “Lock the websites which are in the PC E-Lock database and you added to the filtrate website list”; select “Filtrate Keyword” and the system default is to “Lock websites are of the keyword character from the keyword list and the keyword is “Mail” ” in the list (In that case, mail system in websites would be unavailable for you.). The system default is “Enabled” to “Filtrate Unhealthy Website”, “Filtrate other Websites” and Filtrate Keyword”. It as well provides function to import website or keyword in “.txt” file and one website address or a keyword is for one line. Same website or keywords imported will not be repeated. As follows,



Prompt:

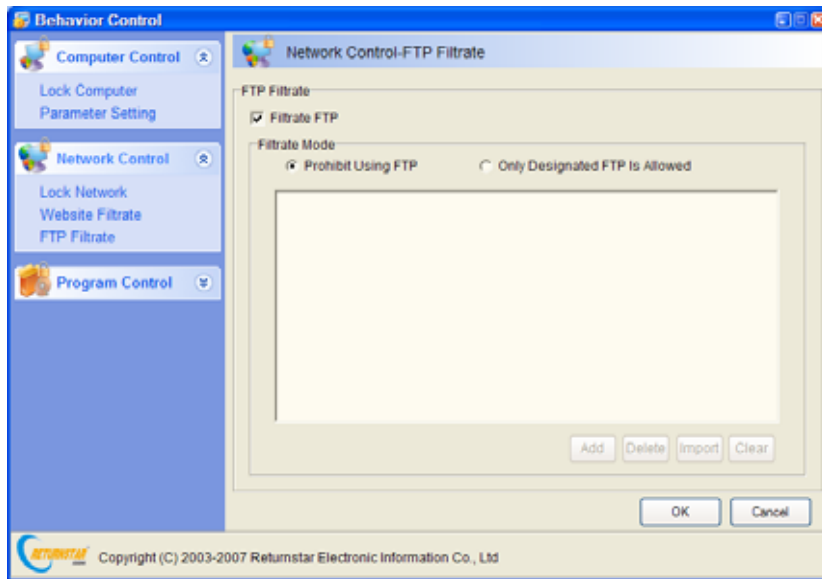
1. The added website must be of the First Class Domain Name. For example, both <http://www.returnstar.com> and <http://www.returnstar.com/index.htm> are of the same Class Domain Name. You must type whole website information, namely, “http://www.” not “www.returnstar.com” or “returnstar.com”. Then all websites including returnstar.com will be forbidden or designated.
2. The default internet homepage must be set as “about: blank”.



4.3.3 FTP Filtrate

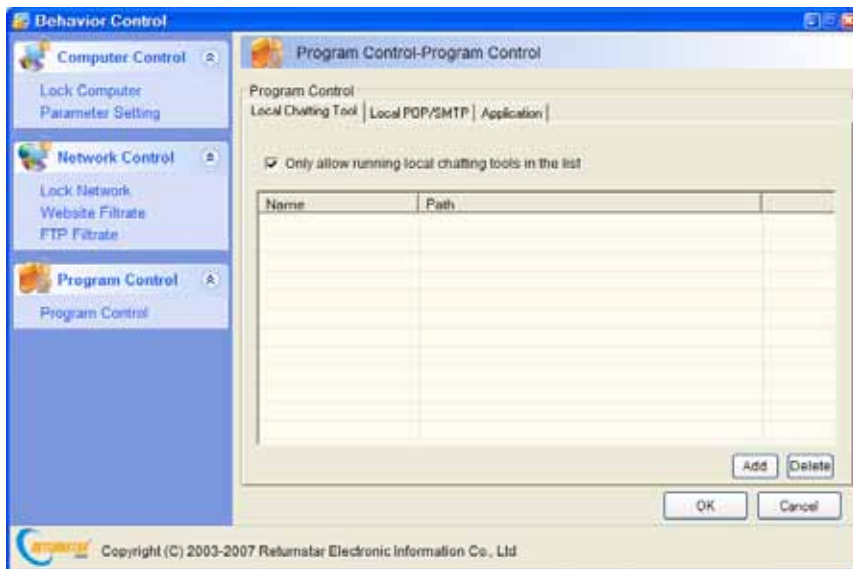
Provide functions of “Only Designated FTP allowed” and “Prohibit Using FTP”. By controlling FTP upload and download, you can effectively control your visiting website character under Controlled Mode. The system default is

“Enabled” to “Prohibit using FTP”. As follows:



4.3.3 Program Control

Provide functions of “Application Control”, “Local Chatting Tool Control”, and “Local POP/SMTP Control”. You can effectively control the program (lock software of computer) under Controlled Mode.



4.3.3.1 Local Chatting Tool Control

Select the function and you can add the local chatting tools you permit to use. The system default is “Enabled” to “Lock local chatting tool existing in PC E-Lock database”.

4.3.3.2 Local POP/SMTP Control

Select the function and you can add the allowing local POP/SMTP you permit to use. The system default is “*Enabled*” to “*Lock local POP/SMTP existing in PC E-Lock database*”.

4.3.3.3 Application Control

Select the function and you can add the applications you permit to use. The default is enabling the program bundled with Windows and Office software etc except games bundled with Windows. Click “*Import Installed Program*” to search the installed programs on the computer automatically, and control the applications according to your requirement. Thus it can effectively control the software under Controlled Mode.



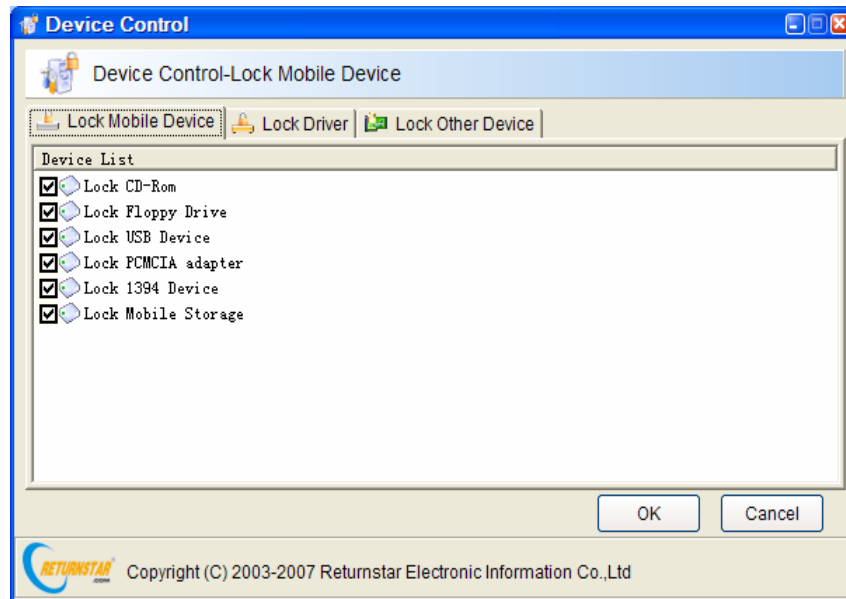
Prompt: You also can add shortcut of any program for program control.

4.4 Device Control

Provide functions of “*Lock Mobile Device*,” “*Lock Drive*” and “*Lock Other Devices*”. With these functions, you can effectively control the hardware using under Controlled Mode. Select devices which you need to lock from provided hardware list then click “*OK*” to save the setting.

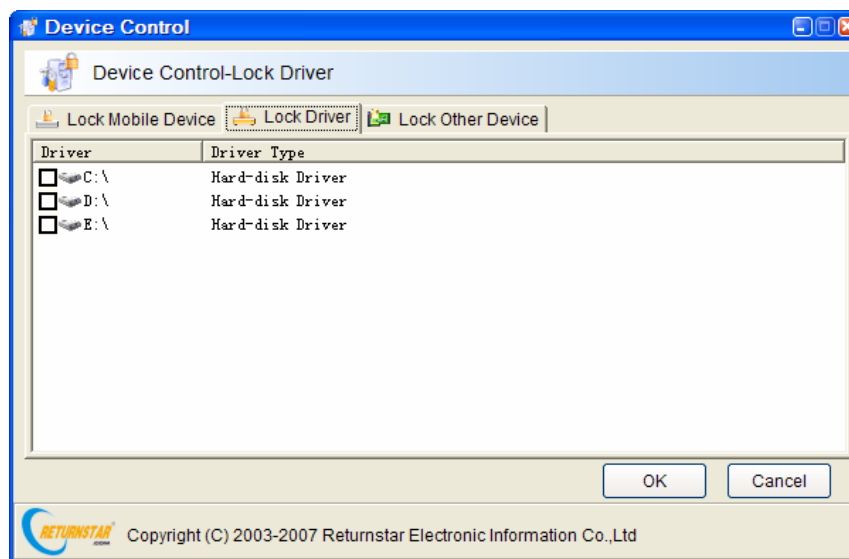
4.4.1 Lock Mobile Device

Provide “*Lock CD –Rom*,” “*Lock Floppy Drive*,” “*Lock USB Device*,” “*Lock PCMCIA Adapter*,” “*Lock 1394 Device*,” and “*Lock Mobile Storage*” and other mobile devices. It effectively control the install or copy of adult, violent or unhealthy software, games, programs and files through such devices and avoid virus, porn-information intrusion, and secret file being revealed under Controlled Mode. The system default is “*Lock all devices*”. As follows,



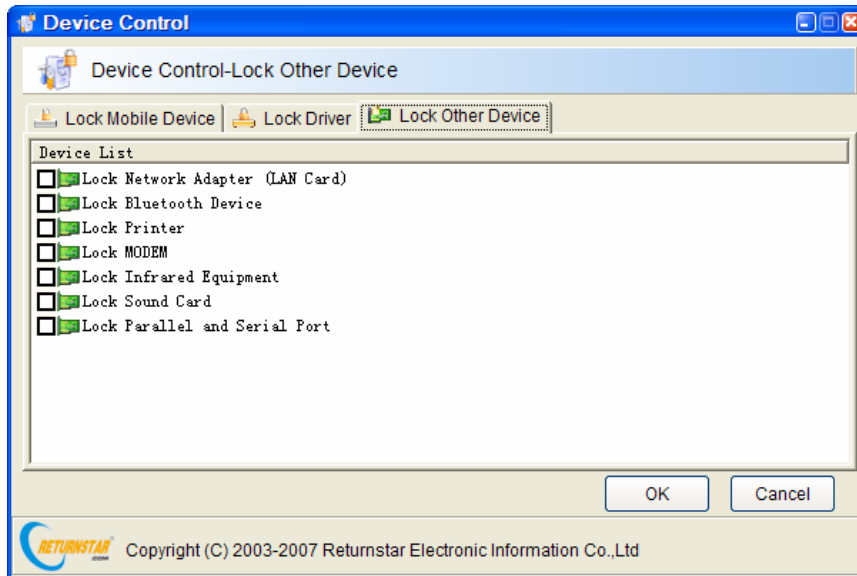
4.4.2 Lock Driver

Provide a list of all current drivers and the extended drivers connected with PC to select. The system default is “Unlock”, as follows,



4.4.3 Lock Other Device

Provide functions of “Lock Network Adapter (LAN card)”, “Lock Bluetooth Device”, “Lock Printer”, “Lock MODEM”, “Lock Infrared Equipment”, “Lock Sound Card”, “Lock Parallel and Serial Port” etc. As follows,



Prompt: No matter which equipment you select, we are setting to unlock any kinds of keyboard and mouse (USB, parallel and serial port or wireless).

4.5 Data Security

Provide functions of “Data Encrypt”, “My Secret Disk” and “Data Crush”. By Data Security, the possibilities of revealing, modifying and deleting the secret data will be effectively removed.

4.5.1 Data Encrypt

Provide two different encrypt methods: “*Local Encrypt*” and “*Mobile Encrypt*”. As follows,

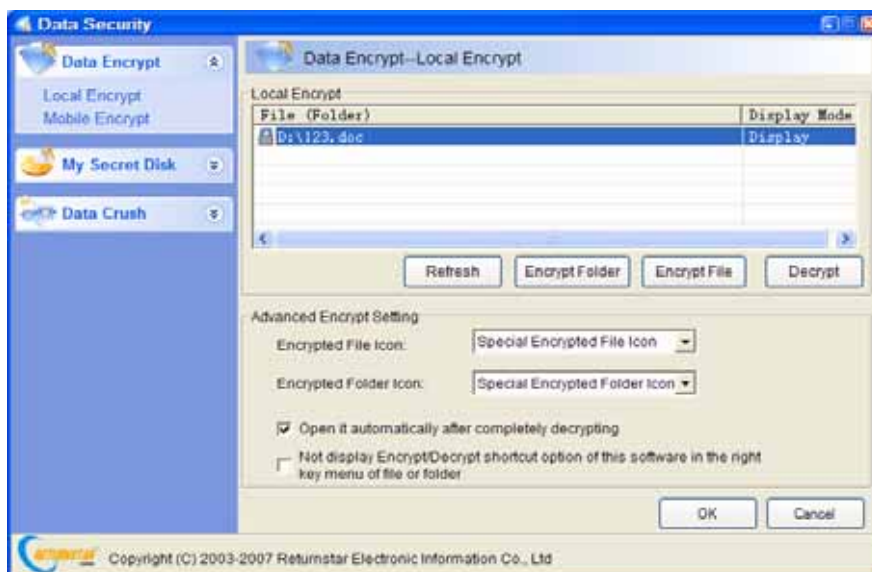
4.5.1.1 Local Encrypt: It is of the highest security.

- Encrypted file or folder will be unable to open or decrypt, when it is renamed or copied to other places.
- Encrypted file or folder can still be found and opened or decrypted from encrypted file (folder) list on the “*Data Encrypt*” Main Menu (see the below figure), after it is deleted.
- If the encrypted file or folder have been cut or deleted, you are unable to open or decrypt them in the new path, but can still find to open or decrypt it

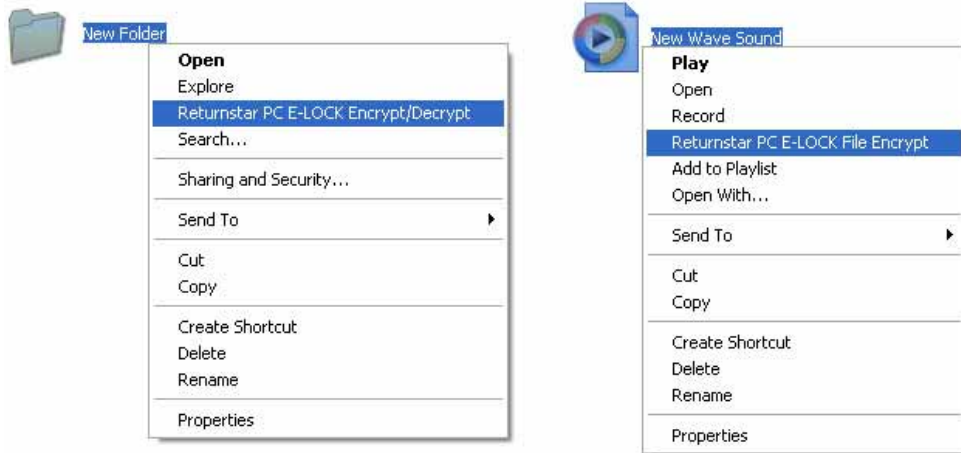
from encrypted file (folder) list on the “Data Encrypt” Main Menu (see the below figure). It can effectively prevent others from using, deleting or modifying the storage path or copying your data in the computer.



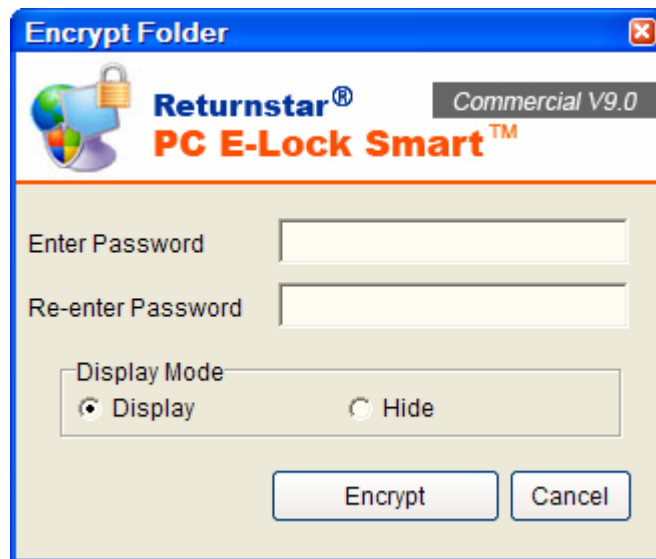
Caution: Press “Fresh” button to re-check it in the list, when closing an encrypted folder or file.



Provide an item list for encrypted file (folder). You can add the item of file (folder) which you need to encrypt to the list (which shows the path and display mode of encrypted file or folder, etc.) by selecting “Add File” or “Add Folder”. You can move the mouse to the file or folder which you need to decrypt at once in the list and click “Decrypt” then input your password in the popup box. Then the file or folder will be open or decrypted. You are also able to encrypt or decrypt the file or folder by clicking “Encrypt” or “Decrypt” shortcut option on the right- key menu of the file or folder in the explorer.



“*Local Encrypt*” has two different display modes: Display and Hide. It means the encrypted file or folder will be displayed or hidden on the Windows explorer. The system default is “*Display*”.





Cautions:

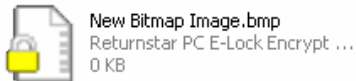
- *If you adopt “Hide” to display the file or folder by “Local Encrypt” you must decrypt it on the “Data Encrypt” Main Menu (see the above figure) since it can not be found on the Explorer,*
- *After reinstalling OS, all encrypted files or folders will keep in an encrypted state and original password. You are able to decode them when re-install the product.*
- *The encrypted folder can not be in the partition where you will re-install OS, otherwise it will be deleted when re-install.*
- *After uninstalling PC E-Lock, the previously encrypted folder is unable to decrypt, moreover keeps encrypted. You are able to decrypt them when re-install the product.*

Design some parameters for users’ convenience as follows,

Encrypted File Icon: Provide three different icons.

- **Windows Standard File Icon**
- **Special Encrypted File Icon**
- **Customized File Icon (The format must be .ICO)**

The system default is “*Special Encrypted File Icon*”.



Encrypted Folder Icon: Provide three different icons.

- **Windows Standard Folder Icon**
- **Special Encrypted Folder Icon**
- **Customized Folder Icon (The format must be .ICO)**

The system default is “*Special Encrypted Folder Icon*”.



Not display Encrypt/ Decode shortcut option in the right- key menu of file or folder: Prevent others from knowing you have installed the product. The system default is “*Display Encrypt/Decrypt shortcut option*”.

Backup original file as “*.RAK” before encryption: Before file encryption, system will automatically backup the file with extension name of “.BAK”. The system default is “*Enabled*”.

Open files or folders automatically after it is decrypted: The system will automatically open the file or folder after being decrypted. The system default is “*Open*”.

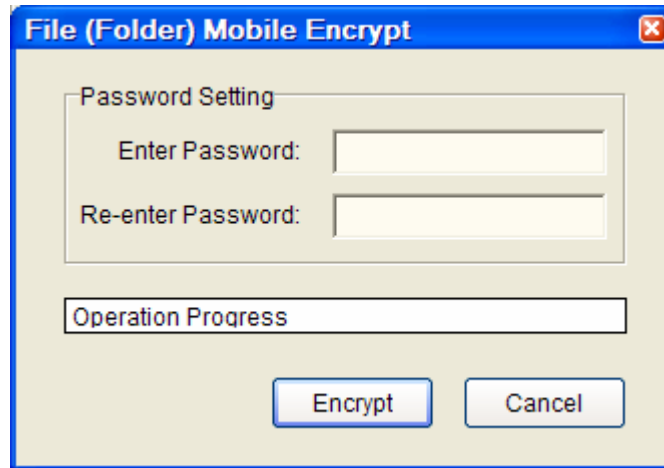
4.5.1.2 Mobile Encrypt

The file or folder encrypted by Local Encrypt is unable to move, so you must use Mobile Encrypt to encrypt the file or folder that you need to move it. It can ensure the security of moving file and folder mostly. The mobile-encrypted file or folder is of the following characteristics:

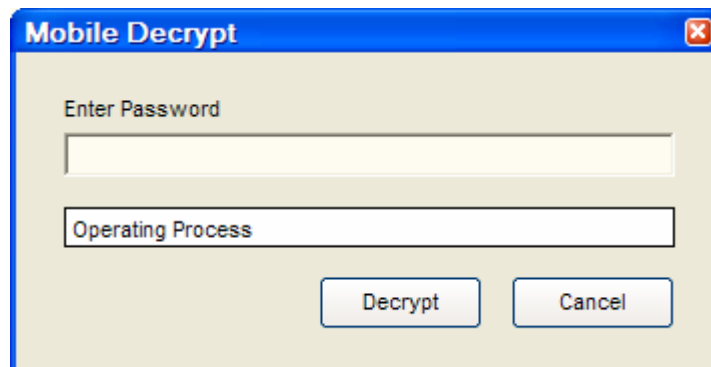
- The encrypted package which has been mobile encrypted is in “*.EXE” format. The file can be deleted, copied, moved to other path or other computers while keeping encrypted.
- Copies of the encrypted package or the moved encrypted package can be open or decrypted in a computer without installing a PC E-Lock.



Click “*Add File*” or “*Add Folder*” to select the file or folder which you need Mobile Encrypt in the popup explorer (The file or folder path will display on the mobile encrypt item). Select “*Delete the original file or folder after being mobile encrypted*” and the system default is “*Deleted*”. Click “*Mobile Encrypt*” and input your password, the file or folder would be mobile encrypted. As follows,



Double-click the mobile encrypted package on Windows Explorer, it will automatically popup the “*Mobile Decrypt*” Box. And then input your password to decrypt. As follows,



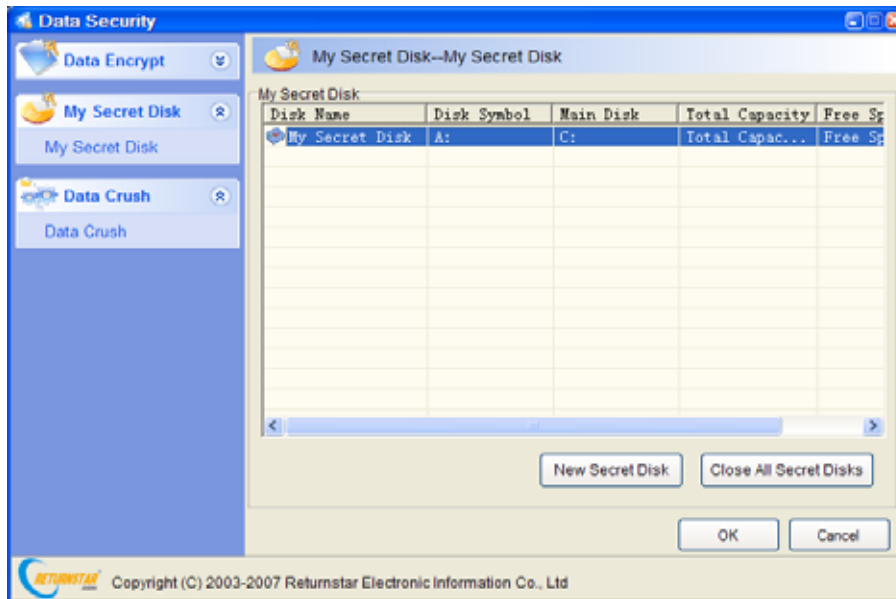


Prompt: (Applicable for Local Encrypt or Mobile Encrypt)

- *The encrypted file is valid under safe mode, DOS and other operating systems.*
- *The encrypt function adopts multiple encrypting methods which combine our exclusive developed encryption technology with the current leading encryption technologies. No matter who is proficient at computer or whichever tools are used, it can not be decrypted. Therefore you must bear your password in mind.*
- *Please do not encrypt the folders such as "Windows", "Program Files", "SYSTEM32", etc which are needed in system. Otherwise it is possible to cause the system error.*
- *The encrypted file or folder is unable to copy, read and write. So it can prevent the virus and Trojan from ruining and attacking.*
- *The encrypted file or folder is unable to be executed, avoiding the potential destroyer using the program. For example, some files or folders get new virus, however, anti-virus software only can identify its path but can not delete them. You can use the function to lock the file or folder with virus and then delete them after anti-virus software upgrade.*
- *Data Encrypt supports to lock any program files such as "*.EXE", etc.*
- *If the user locked A file or A folder, then A file or A folder shortcut will be ineffective.*

4.5.2 My Secret Disk

It is of the so-called file safe function. You can set up one or more new secret partitions in any original partition with free space and copy the confidential data or save them to these secret disks, which can prevent others from seeing the disk or using data in it under Controlled Mode. You can create, set, and manage multiple secret disks in it. As follows,



4.5.2.1 New Secret Disk

Click “*New Secret Disk*”, the system will popup the New Secret Disk Setting Dialog box. As follows,



Set your new Secret Disk, including “*Secret Disk Name*” (support names in various kinds of language, but these names should not exceed 16 Chinese characters or 32 characters, and the detailed restriction is same as “*WINDOWS partition naming*”, “*Secret Disk Symbol*”, “*New Space on*” (means to select the main disk in which you set up the new secret disk, and we provide all current disk symbol and corresponding free space for your selection), and “*Secret Disk Password*” in this dialog box. Then click “*OK*” to display new Secret Disk item on the “*Secret Disk List*”.



Prompt:

- *The secret disk is one or more partitions you set up in previous partition, which means that it is based on the original partition. We can consider it as “partition in partition”. The space of the original partition will be reduced when adding files in the secret disk.*
- *After system reinstall or software uninstall, all the secret disk and data in it will not be destroyed so long as you do not re-part or change partition format. You will find the secret disk and data after you re-install this software.*
- *You can set up several secret disks. These secret disks can not use the same name and disk symbol, but can be set up on the same partition. All secret disks’ passwords would be different.*
- *No need to format it, after setting up your secret disk. The partition is in the same format as the original partition.*

Provide secret disk list on “*My Secret Disk*” setting interface, which lists all current established secret disk items (displaying Secret Disk Name, Secret Disk Symbol, Main Disk, Used Space, and Free Space, etc.). Move the mouse to the secret disk item on the list and right-click it, you will see the pull-down menu and then select the following options to operate the secret disk:

4.5.2.1.1 Open

Click “*Open*” and input your password in the popup box. The secret disk explorer will automatically open the corresponding secret disk. You can operate them in the secret disk explorer as in the system explorer. You will find the secret disk symbol in Windows explorer.



Important statement: *The deleted files or folders in the secret disk will never be in the system’s Recycle Bin. Such design is to guarantee your private data security. The deletion of files or folders in secret disk is like “Data Crush”. (Refer to the next section “Data Crush”)*

4.5.2.1.2 Close

Click “*Close*” (or switch to Controlled Mode) the Secret Disk symbol will disappear in Windows explorer.

4.5.2.1.3 Delete

Click “Delete” and input your password in popup dialog box to delete the disk.



Important Statement: After deleting the secret disk, the data will be crushed and not exist on the Recycle Bin. Such design is to guarantee your private data security. The secret disk is deleted like “Data Crush”. (Refer to the next section “Data Crush”), and then the used space will be released to the main disk

4.5.2.1.4 Clear all Data

Click “Clear all Data” and input your password in popup dialog box to clear up all data in the disk.



Important statement: After clearing up data in the secret disk, those data will never show up on the Recycle Bin. Such design is to guarantee your private data security. The secret disk is emptied like “Data Crush”. (Refer to the next section “Data Crush”)

4.5.2.1.5 Secret Disk Setting

Click “Secret Disk Setting” to appear the Secret Disk Setup Interface, you can reset the parameter and password.



Prompt: Please confirm the free space of the new main disk must be larger than the used space of the secret disk before you change the main disk, otherwise the data transfer will fail!

4.5.2.1.6 Import Data

Click “Import Data” and input your password in popup dialog box, then select the folder or file you want to move on the popup explorer. The folder or file will be cut into the secret disk.

4.5.1.2.7 Export all Data

Click “Export all Data” and input your password in popup dialog box, then select the catalog or file you want to move on the popup explorer. All data in this secret disk will be cut into the secret disk.

4.5.1.2.8 Close all Secret Disks

Click “Close all Secret Disks” and all open secret disks will be closed.



Database Encrypt:

- *Backup the database files*
- *Set up the private secret disk such as Z disk*
- *Reinstall management software and set the install or database default directory to the private secret disk (Z disk)*
- *When you do not login to the Administrator Mode, the management software will prompt error, and the database is unable to be open. You can use the software normally and open the database when you login To the Administrator Mode.*

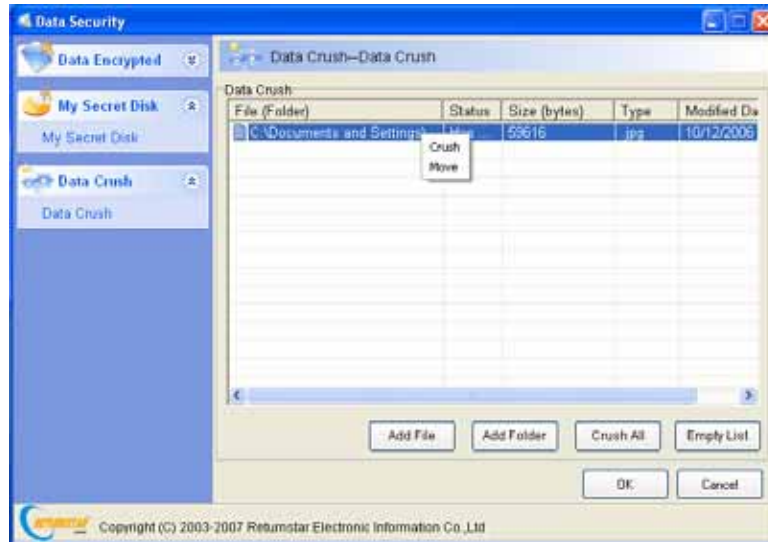


Data Multi-encrypt:

- *Mobile encrypt data if you need to move it*
- *Save the data to my secret disk*
- *Encrypt the data file*
- *Encrypt the catalog where the data file is again*
- *After that your data has multiple protections. No one can guess your password easily, and say nothing of decoding. Certainly you can also use the compress software such as WINRAR, etc. to compress and encrypt it again.*

4.5.3 Data Crush

Provide item list of the file (folder) which is to be crushed. You can select “Add file” or “Add folder” to add the file (folder) on the list (display Path, Status, Size, Type, Time etc of file or folder) . Move the mouse to the file or folder which you want to crush in the list and right-click to appear the pull-down menu, and then click “Crush” to crush the file or folder, or click “Move” to move the file or folder item from the list. Click “Crush All” at the lower corner of list to crush all files or folders. Click “Empty List” to remove all files or folders from the list. The crushed file or folder will display “Crushed” on the list as follows,



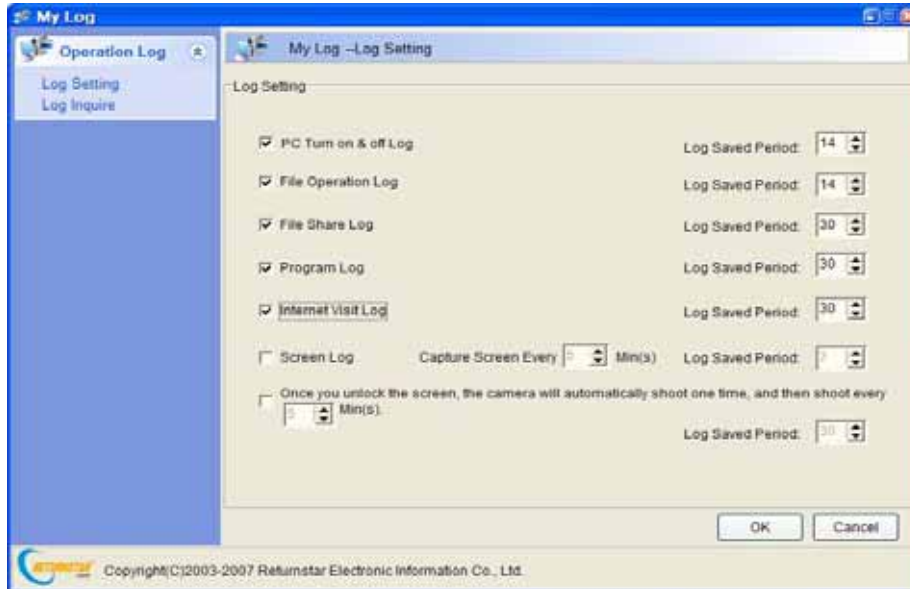
Important Statement: Data Crush function can not only delete the file and folder, but also clear up the file and folder's information on the magnetic track thoroughly. The crushed file or folder can't be recovered, even using the "Final Data" tool. Any behaviors trying to find out and recover the lost information will fail, so you should be cautious when executing the operation.

4.6 My Log

Provide "Setting", "Inquire", "Clearing up" and "Export" functions for "Start PC Log", "File Operation Log", "File Share Log", "Program monitor Log", "Website Monitor Log", "Screen monitor Log" and "User Monitor Log". By log setting, you can effectively monitor the computer and grasp the administrated user's habit, discover and improve the scientificity and rationality of PC E-Lock management setting under Controlled Mode.

4.6.1 Log Setting

Set the saved period of Monitor Log. As follows:

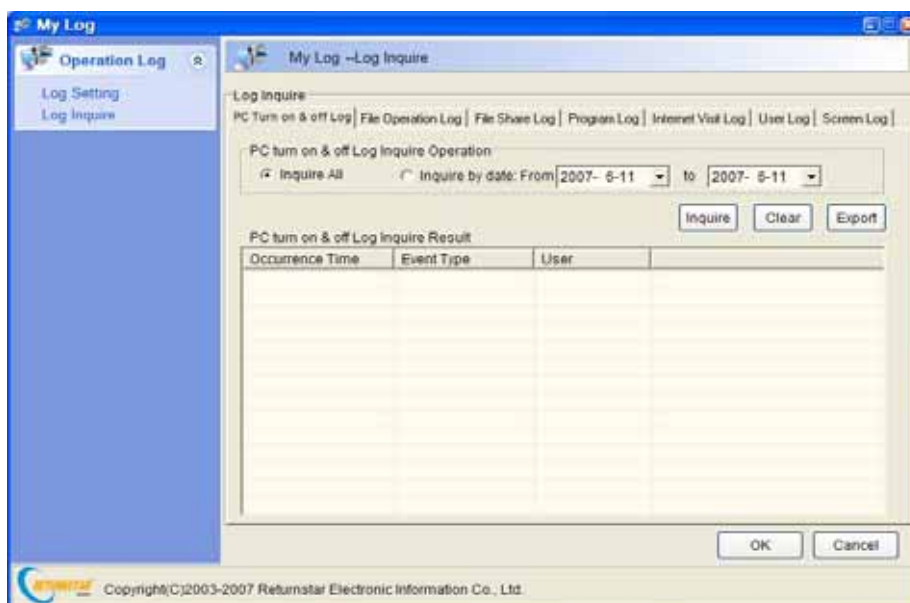


4.6.2 Log Inquire

Provide “*Inquire*”, “*Clear*” and “*Export*” for saved Record of Monitor Log according to the schedule. Click “*Inquire*” button to refresh the record in the current list. Click “*Clear*” button to clear up the current record. Click “*Export*” button to export the record into “.txt” file.

4.6.3 PC Turn on & off Log

Convenient to inquire about the details recorded under Controlled Mode, including PC Start, Logout and terminate Schedule, Login Schedule and Login User Name etc. It can save the record up for 0-14 days. The system default is 14 days and “*Enabled*”. As follows,



4.6.4 File Operation Log

Convenient to inquire about the details of file operation recorded under Controlled mode, including Occurrence Time, Affair Style, Details etc, (such as “Copy”, “Delete”, “Move”, “Rename”, “Open”, “Close” etc). It can save the record for 0-14 days. The system default is 14 days and “Enabled”.

4.6.5 File Share Log

Convenient to inquire about the details of file or folder share recorded under Controlled Mode, including Visiting Time, visitor and Visit content etc. It can save the record for 0-30 days. The system default is 30 days and “Enabled”.

4.6.6 Program Log

Convenient to inquire about the details of program running recorded under Controlled Mode, including Occurrence Time, Program Name and Affair Type etc. It can save the record up for 0-30 days. The system default is 30 days and “Enabled”.

4.6.7 Internet Visit Log

Inquire conveniently about the details of internet visiting recorded under Controlled Mode, including Occurrence Time, Website Address and Type etc. It can save the record for 0-30 days. The system default is 30 days and “Enabled”.

4.6.8 User Log

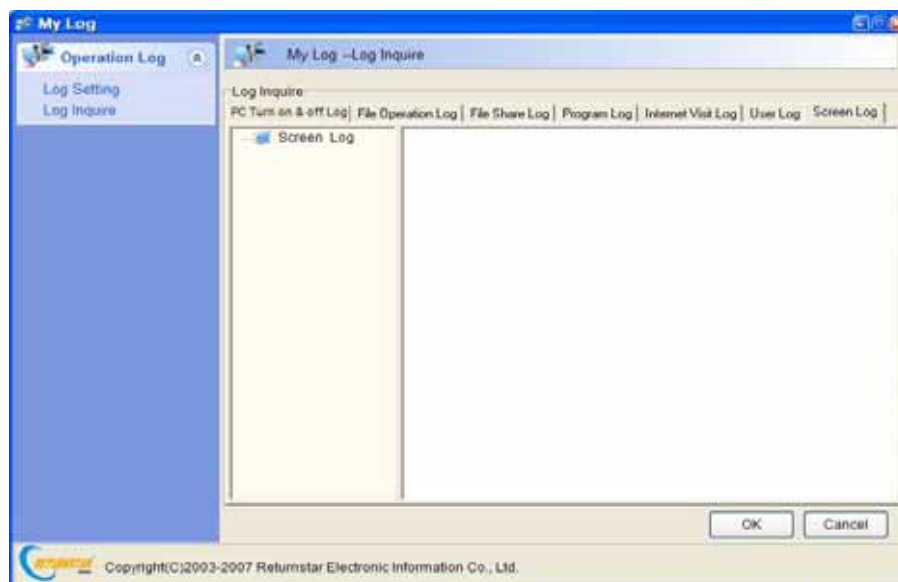
Convenient to inquire about the user’s photo captured by the system and recorded under Controlled Mode in detail. If someone uses your computer or input the locked password to enter into your computer when you leave, the webcam will automatically take a photo of user every other 5-60 minute, and the system default is 5 minutes. It can save the record up to 30 days. The system default is 30 days and “Disabled”. Since that the users’ photos will occupy a large MD space, it is recommended to delete photos by selecting “delete” on the right-key menu of the file or folder in the left file list after you check it every time.



Prompt: For “User Monitor Log”, the webcam must be installed previously and adjusted to your face. Please adjust focus in order to capture your face clearly!

4.6.9 Screen Log

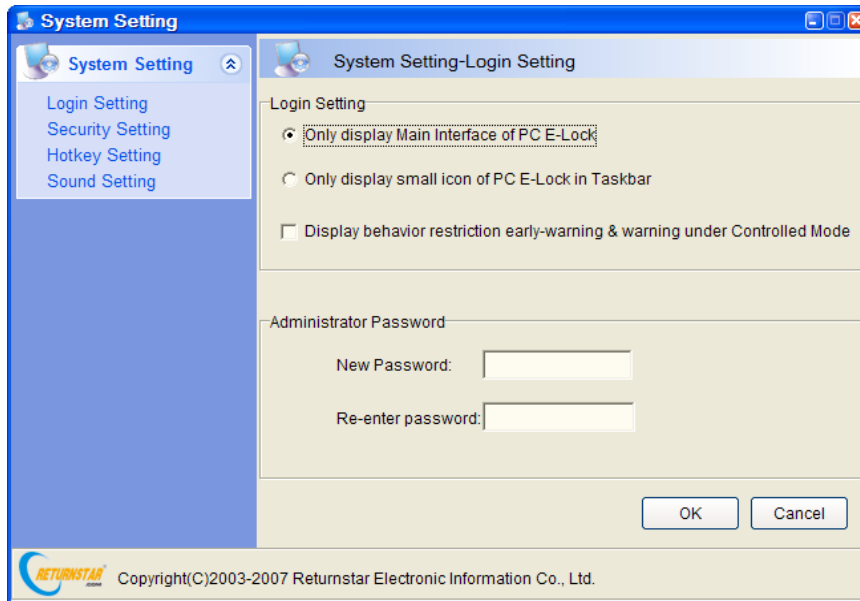
Convenient to inquire about the screen image recorded under the Controlled mode. We can set to capture every other 5-60 minute, (the system default is 5 minutes); and the record can be saved for 0-7 days (the system default is 7 days and “Disabled”). Since that the screen records need for large MD space, it is recommended to delete records by selecting “delete” on the right-key menu of the file or folder in the left file list after you check it every time.



4.7 System Setting

4.7.1 Login Setting

Set the product login method and administrator password. As follows,



4.7.1.1 Only display Main Interface of PC E-Lock

Only the Main Interface is displayed when logging in. The system default is “*Enabled*”.

4.7.1.2 Only display small icon of PC E-Lock in Taskbar

Only the small icon is displayed in the taskbar at the lower-right corner of the desktop when login. Recommend to choose this function for your convenience of operation after this product installed. The system default is “*Disabled*”.

4.7.1.3 Display behavior restriction early-warning & warning under Controlled Mode

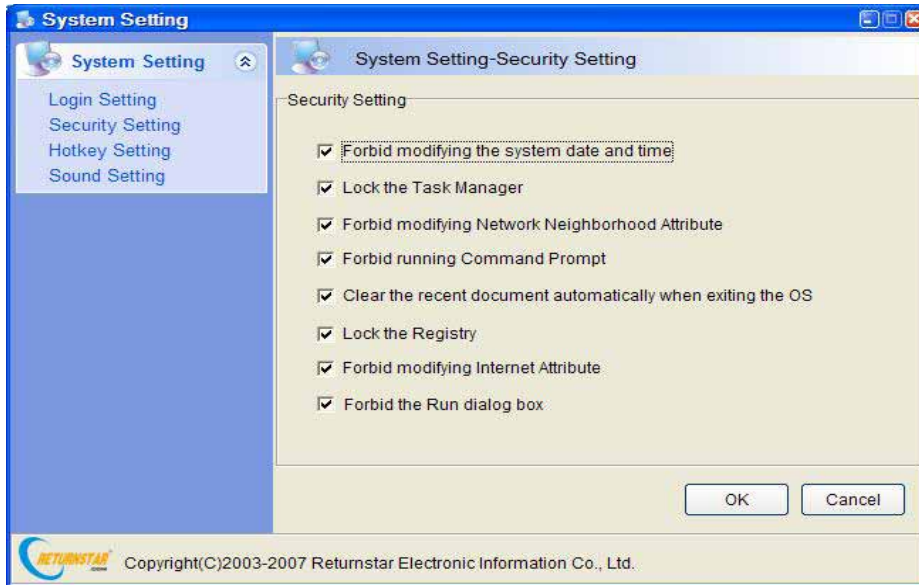
Behavior restriction warning prompt will be displayed in the middle of the screen under Controlled Mode. The system default is “*Disabled*”.

4.7.1.4 Administrator Password

Modify the administrator password, which is required when to login.

4. 7.2 Security Setting

Restrict others from using the computer system to ensure the system security and PC E-Lock normal working by this setting. As follows,



4.7.2.1 Forbid modifying the system date and time

Forbid modifying the system date and time under Controlled Mode. The system default is *“Enabled”*.



Prompt: Strongly recommend setting up BIOS password to prevent BIOS time from being modified!

4.7.2.2 Lock the Registry

Forbid opening the system registry under Controlled Mode. The system default is *“Enabled”*.

4.7.2.3 Lock the Task Manager

Forbid opening the task manager under Controlled Mode. The system default is *“Enabled”*.

4.7.2.4 Forbid modifying Internet Attribute

Forbid modifying the system Internet Attribute under Controlled Mode. The system default is *“Enabled”*.

4.7.2.5 Forbid modifying Network Neighborhood Attribute

Forbid modifying the Network Neighborhood Attribute under Controlled Mode. The system default is “*Enabled*”.

4.7.2.6 Forbid the Run dialog box

Forbid running the system dialog box under Controlled Mode. The system default is “*Enabled*”.

4.7.2.7 Forbid running Command Prompt

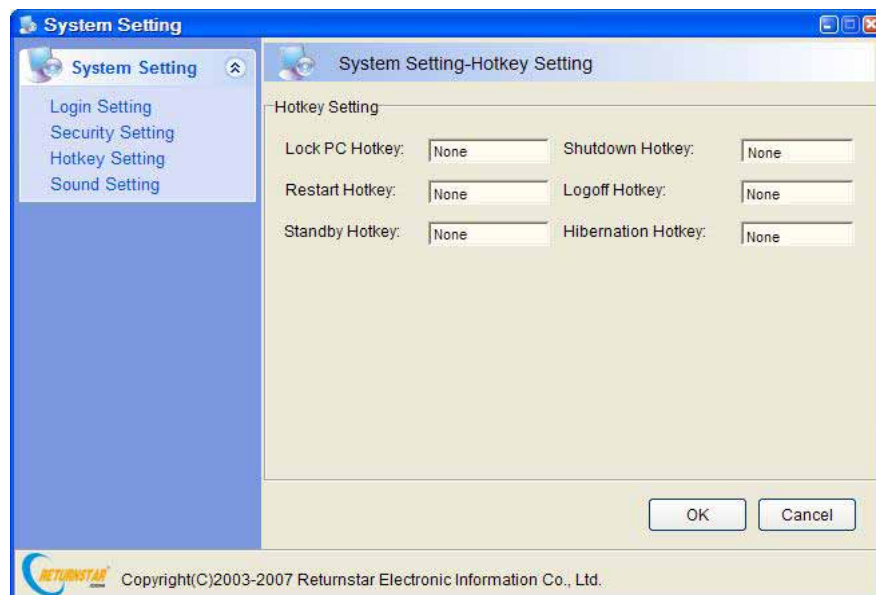
Forbid running the system command prompt under Controlled Mode. The system default is “*Enabled*”.

4.7.2.8 Clear the recent document automatically when exiting the OS

Clear the recent documents automatically when exiting the OS. The system default is “*Enabled*”.

4.7.3 Hotkey Setting

Set up handy Hotkey to control system, for your convenience. To set up hot key, press the one which you want to set up into this hotkey box. (If the hotkey has been occupied to control other program, the setting will be disabled). As follows:



4.7.3.1 Lock PC Hotkey

Under Administrator Mode, press this hotkey to lock your computer directly

until the administrator unlocks it.

4.7.3.2 Shutdown Hotkey

Under Administrator Mode, press this hotkey to shut down your computer directly.

4.7.3.3 Restart Hotkey

Under Administrator Mode, press this hotkey to restart your computer directly.

4.7.3.4 Logoff Hotkey

Under Administrator Mode, press this hotkey to log off your computer directly.

4.7.3.5 Standby Hotkey

Under Administrator Mode, press this hotkey to make your computer standby directly.

4.7.3.6 Hibernation Hotkey

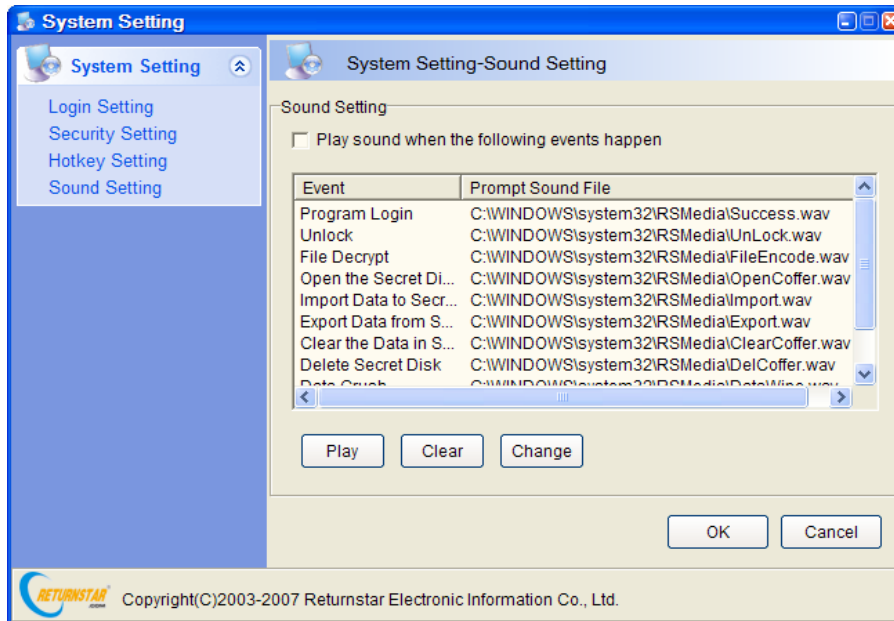
Under Administrator Mode, press this hotkey to make your computer hibernate.



Prompt: *If no need to set up the above hotkeys temporarily, press "Space" key in the hotkey box directly.*

4.7.4 Sound Setting

Set the sound prompt when some events of PC E-Lock happen (including "Program Login", "Unlock PC", "Decrypt File (Folder)", "Open the Secret Disk", "Import the Data to Secret Disks", "Export the Data from Secret Disks", "Clear the Secret Disk", "Delete Secret Disks", "Data Crush", "Incorrect Password Input" etc). The sound file format only can be ".wav". The system has provided the default sound for these events.



4.7.4.1 Play

Select the event of which you want to pre-hear the sound prompt from the events list, and then click “*Play*”, the system will play the corresponding prompt sound for you.

4.7.4.2 Clear

Select the event of which you want to delete the sound from the event list, and then click “*Clear*”, the system will clear up the corresponding sound for you. You will not hear the prompt sound when the event occurs.

4.7.4.3 Change

Select the event of which you want to change the sound from the event list, and then click “*Change*”; you can choose the sound in your favor in the popup window.

Chapter 5 Upgrade

We provide two ways to upgrade the product:

- Click “*Upgrade*” option on the main interface or right key menu of small icon in taskbar, and then system will automatically prompt that upgrade package is found and now it is upgrading (subject to version NO. and time of upgrade package). It is unnecessary to uninstall the old version’s software when upgrade.



Prompt: *The function is only provided for registered version.*

- You have to uninstall the old version, and download the new version to install from our website: www.recoverystar.com if this product has been significantly improved and upgraded.

Chapter 6 Notice

6.1 The product can not be used under Windows 95, Windows NT 3.51, and Windows NT 4.0.

6.2 All functions of the product can be used separately or be multiple set, but please note that the function of “Lock Computer” takes the priority.

6.3 It's not allowed to install another product of the same model on the same system.

6.4 You have to install the product for each operating system if your PC is installed with multiple operating systems

6.5 Please reinstall the product under newly reinstalled operating system at once, in order to guarantee normal using.

6.6 We designed four passwords for this product: Program Administrator Password, Lock File (folder) Password, My Secret Disk Password and Super Password. They support blank password, except the Super Password. Super Password is the registry number and is applicable in Program Administrator Password, Lock File (folder) Password, and thus you should save and keep your registry number confidential.



Important Statement: *The product series has been significantly upgraded. If your version is under V9.0, uninstall it after decrypting the files (folders) and secret disk and then install the new version V9.0.*

Chapter 7 FAQ

1. Is there any product with similar function in the market at present?

A: There is no similar product with such high security and efficiency in the market at present. Maybe there are some products (pure software / software+ hardware) achieve some functions but with following shortcomings:

- Easy to be decrypted.
- Easy to be uninstalled and deleted by administrator.
- Easy to terminate or delete its program in the registry and task manager.
- Invalid under the safe mode.

Please be cautious to purchase.

Appendix: Purchase and Register

Trial: You can download our Returnstar PC E-Lock software package to install from our website. (<http://www.recoverystar.com>), and you can get a trial for 30 times. The trial time is subject to your booting PC E-Lock. After 30 times, if you want to go on, you must register the product.

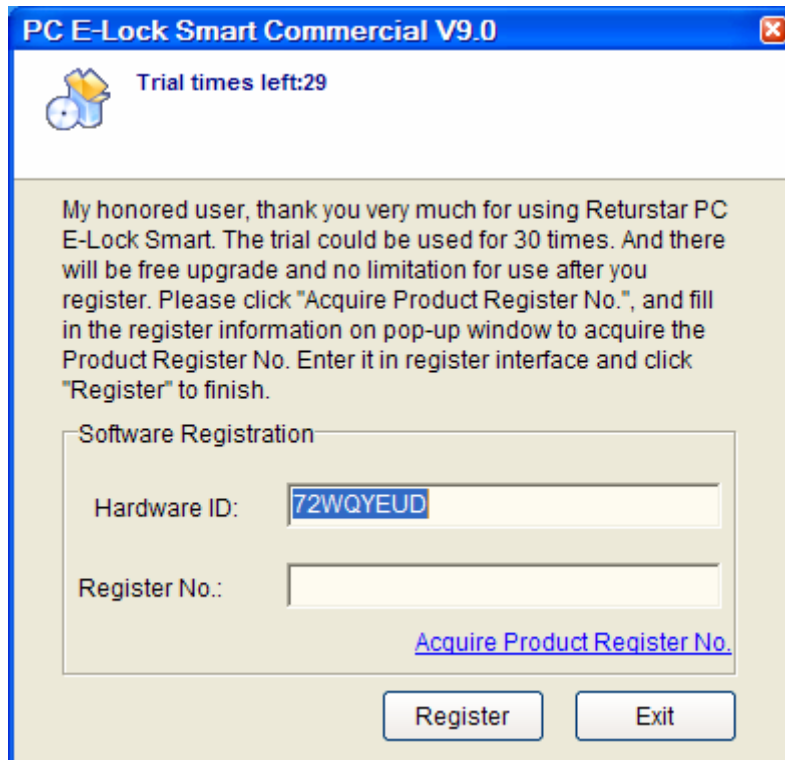
Purchase: Contact Returnstar Electronic Information Co., Ltd headquarter or our business agents to purchase original software. A full set of software includes Installation CD, Product Serial Number and User Manual. Or you can get Product Serial Number through online purchase at large shareware website.

Register: No need to un-install a trial version after purchasing the software. Enter the Product Register Interface and click "*Obtain Product Registration No.*"; then input your product SN and Hardware ID Code in the popup box to acquire Product Registration No. Write down your Product Registration No. and input it in the Product Register Interface, and click "Register" button to finish registration. If your 30-time trial ends, it will prompt you to input Product Register Number after you start PC every time. You can input Product Register Number in the prompt box and press "Enter" to finish.

Besides you can use your E-mail or telephone to acquire Product Register Number manually. Our detailed information is as below:

Email: master@recoverystar.com

Telephone: +86-591-83385086



Caution: Please be sure to register after you install the product. The unregistered user only can use 30 times, by contraries the registered user can use without any limitation and get free upgrade. If your PC E-Lock Smart is not registered, and your trial is up, moreover you don't want to use this product, then you have to uninstall this product. You can uninstall directly without login the product. Please note this product is unable to use and will prompt "Your trial times have ended!" if you reinstall PC E-Lock.