

Market provider and Technology support: www.cosolid.com

Cosolid[®]
PC E-LOCK PRO
Manual



Copyright(C) 2007 COSOLID AB

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

Tel: +46-8-6640729

Fax: +46-8-6640739

E-mail: support@cosolid.com

Copyright Declaration I

While Cosolid AB grants the using rights of this product program to you, you need to ensure that, other than license conditions permitted in this agreement, you should never use, reproduce, imitate, copy, lease, rent, sell, modify, de-compile, disassemble or conduct other reverse engineering on the program, and you should never transfer the licensed programs or any subset of these programs to others. Any unauthorized usage of this program will lead to immediate and automatic termination of this license agreement, and may lead to criminal and/or civil lawsuits.

1. Use this product on only one computer;
2. On the condition that the third party agrees on the items and conditions in this agreement, you can transfer this product and related license agreement to a third party. If transfer occurs, all copies of the original documents and related documents must be transferred to the third party. All copies that have not been transferred should be destroyed.
3. Use this product in a multi-user environment or network system only when one of the following conditions is met:
 - This product is publicly licensed for use in a multi-user environment or network system.
 - All nodes and terminals have purchased the usage license for this product.

Copyright and ownership:

Copyright, trademark and / or other property ownership laws protect all text, photos, graphics, audio and/or video materials included with this product. Without the permission of Cosolid AB the above information shall not be directly or indirectly published or broadcast in any media publication, shall not be re-written or re-published for broadcasting or publication purposes, and shall not be used for any commercial purpose.

To provide better services, Cosolid AB has the right to automatically modify any images, photographs, animation, video, audio, music, text, additional procedures and accompanying help materials included in the product when necessary through online or other means. Cosolid AB reserves these rights. Without our permission, users are forbidden to conduct reverse engineering, decompiling or disassembling on this kind of software program.

The products, documents and related software programs are protected by copyright laws, and also by national copyright laws and international treaty provision protection laws. You should not remove the copyright declaration from the products. Furthermore, you should produce a copy of the copyright declaration for any copies (either partially or in full) of the products. Also, you should agree to prevent any illegal copies of the products and documents.

After-sales warranty:

Cosolid AB warrants that there exist no material or craftwork defects in the software carriers under normal use, within 90 days after the date of sales. If verifying such defects do exist, Cosolid AB is fully response for exchange of the software carriers. And this is the only

compensation route for you in this situation. After-sales warranty is not valid for carrier flaws caused by accidents, improper using or incorrect applications. The exchange of carriers is protected for the last day of the original warranty period, or protected in the following 30 days. The longer time period takes precedence.

None of responsibilities:

In addition to the contents described above, any other forms of after-sales warranty are not valid for the products.

Limited liabilities:

The above warranties, which are implied or clearly described, are the full contents of after-sales warranty for special commercial or adaptive purposes. Whether this agreement is maintained or not, Cosolid AB and its agents or salesmen are not responsible for any profit loss, availability reduction, business interruption, and other kinds of indirect, special, incident or inevitable detriments, or claims for compensation from other parties caused by use of this product. Even if Cosolid AB has been notified of these circumstances, it is still not responsible for this.

Termination of License:

If you violate any item or conditions of this agreement, Cosolid AB has the right to terminate this license at any time necessary. When the license is terminated, you must immediately destroy all copies of this product and related documents. Otherwise, you should return all materials to Cosolid AB.

Applicable laws:

<Intellectual, Property, Protection, and Ordinance>,

Copyright Law, Patent Law, and equal not mentioned laws

Other provisions:

Both parties to this agreement have no other authorities covering the agreed items and other related completed agreements, which are specified in this agreement. If any item of this agreement is completely or partially invalid for any reason, the remaining items in this agreement will remain valid and have a constraining effect.

This manual is for general-purpose use. If any contents or product specification in the manual has changed, please accept our apologies in advance for not providing you with further notice.

Copyright Declaration part II

Your purchasing of this product does not mean Cosolid AB 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 printing material, and any copies made in authorization of Cosolid AB are products of Cosolid AB, and their Intellectual Property are owned by Cosolid AB and their partners and manufactures. The name of this product and all its copies are consistent in CD and the manual. The framework, organization and source code of this product are Cosolid AB's and their manufactures valuable commercial secret and may not be transferred. This product is protected by PRC Copyright Law, related international treaties, 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 Cosolid AB., You are allowed to use one product on one computer only. Any reverses engineering, re-compiling, and decoding of this product, and retrieving the source code of the product by other ways is also prohibited.

Cosolid AB, Cosolid PC E-LOCK PRO is the registered trademark of Cosolid AB. Any modification of Copyright marks, product names and brand names of this product and its copies is strictly prohibited.

Cosolid AB. 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 any time without notice.

Copyright©2007 Cosolid AB

Notices: This manual is applicable to Cosolid E-LOCK PRO

Windows® is a registered brand by Microsoft Cooperation

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. Cosolid AB 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. Cosolid AB. 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 FDIS/MBR, repartitioning, or low formatting after boot from FD or CD. Otherwise this company assumes no liability for all losses arising here from, 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 Cosolid AB. Otherwise this company assumes no liability for all losses arising here from, express or implied.
 - Regular backup of important data is still necessary when using this product. Cosolid AB does not undertake any compensation responsibility for any losses of HD arising from the prompt sufficient backup.

Chapter 1 Product Introduction

Cosolid PC E-Lock Professional is a product suite for behavior control and security management, it is researched and developed by Cosolid AB PARTNERS for many years hard working.

PC E-LOCK Professional: It is convenient for other consuming group to use in different environment and management habit and warranties the effective management when using same computer in different environments.

Cosolid AB has become 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 behavior control and security management on computer for computer user and administer, and solve the key problems on computer management which disturbing PC users all over the world.

This is an installing and operating manual for COSOLID ® PC ELOCK™ PRO.

Chapter 2 Product Characters

Cosolid PC E-Lock Pro Version has the following strong characters:

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

2.2 Support Windows 2000/XP/2003/Vista OS, it is compatible with any hardware and software when installing and using.

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

2.4 Avoid deleting and terminating program 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.

Notice:

1. The product cannot be used under the Windows 95, Windows NT 3.51, and Windows NT 4.0.

2. All functions of the product can be used separately and multiple set, but please note the function of "*Lock Computer*" has the priority to work.

3. It is not allowed to install the same product with same type on the same system.

4. You have to install the product for each operation system as your PC with multi-operating systems.

5. Please reinstall the product under newly installed operation system at once, in order to guarantee normal using.

6. We designed three passwords for this product: Program Administrator Password, Lock File (folder) Password and My Secret Disk Password. It supports blank password at the same time. You must preserve and secure all kinds of password because the password, administrator password, PC E-Lock smart and your PC are bind together.

Chapter 3 Product Install and Uninstall

3.1 System Requirements:

Ensure your PC has the following characters:

- USB 1.1 or above
- 80X86 compatible computer systems
- More than 500 MB HDD free space and more than 32MB memory
- Operating System: Windows 2000/XP/2003/Vista
- Make sure you have installed LAN Card in the computer.

3.2 Product Install

Insert the USB key into a USB port and then run the program “SETUP.EXE” in the driver CD to install this product. Finish setup according to the prompt.

After finished install, restart the computer and plug in the USB key, then the product Main Interface will be automatically popup, As follows:



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.

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

Chapter 4 Product Usage

4.1 Work Mode

This product has two work modes: Administer Mode and Control Mode.

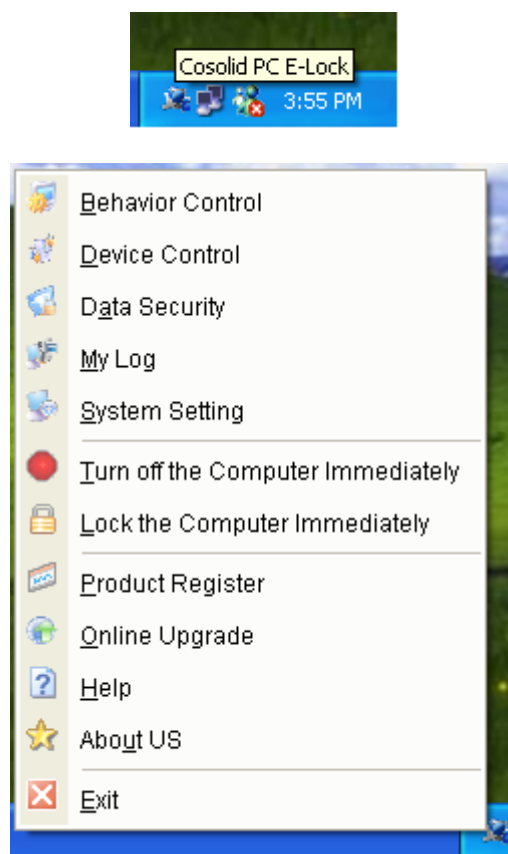
Administer Mode: The computer can be used without any limitation. This is non-control mode. You can conduct functions setting under administer mode.

Control Mode: The program will control the operating system according to your setting. This is control mode.

Switch Work Mode: Two work modes can be switched by plugging and unplugging USB key.

4.2 Product Login

Plug in the USB key, Product Logon Window will be automatically popup. Input the administrator password in the box, and click "OK" to directly enter into Main Menu, or display small icon at the right down corner of taskbar. Login is successful. Double-click the small icon in the taskbar to enter into Main Menu, or right-click the small icon to display the following shortcut menu,



Note: "Data Security" and "My Log" can only be used under the Administer Mode.

4.3.1.2 Behavior Setting

Stipulate when computer will be automatically locked, and what it will do when locked or after locked. It is a very important measure for Behavior Control.

Lock the computer automatically after switch to the controlled mode: Once this function selected, the computer will be automatically locked after switch to the controlled mode. The system default is “*Disabled*”.

Lock the computer automatically after entered into the OS: After entered into OS, the system will automatically lock the computer. The system default is “*Disabled*”.

Automatically turn off computer in [] minutes after locked the computer: Once the function selected, computer will automatically turn into PC E-Lock Screen Saver in any ways at any time, and turn off the computer in 0-60 minutes. The system default is 60 minutes and “*Enabled*”.

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

Have a break of [] minutes after an interval of [] minutes: To protect eyesight and adjust the sitting posture, break will be made for 1-30 minutes for users after an interval of 1-90 minutes when computer used. The system default is “*Break for 10 minutes after an interval of 45 minutes*”. As soon as the using time is arrived, it will automatically turn into the PC E-Lock Screen Saver. At that time, if someone forces to shut down the PC, restart it will be result in automatic entering into the PC E-Lock Screen Saver. Once the break time is over, it will return to the computer using status automatically. The system default is “*Enabled*”.

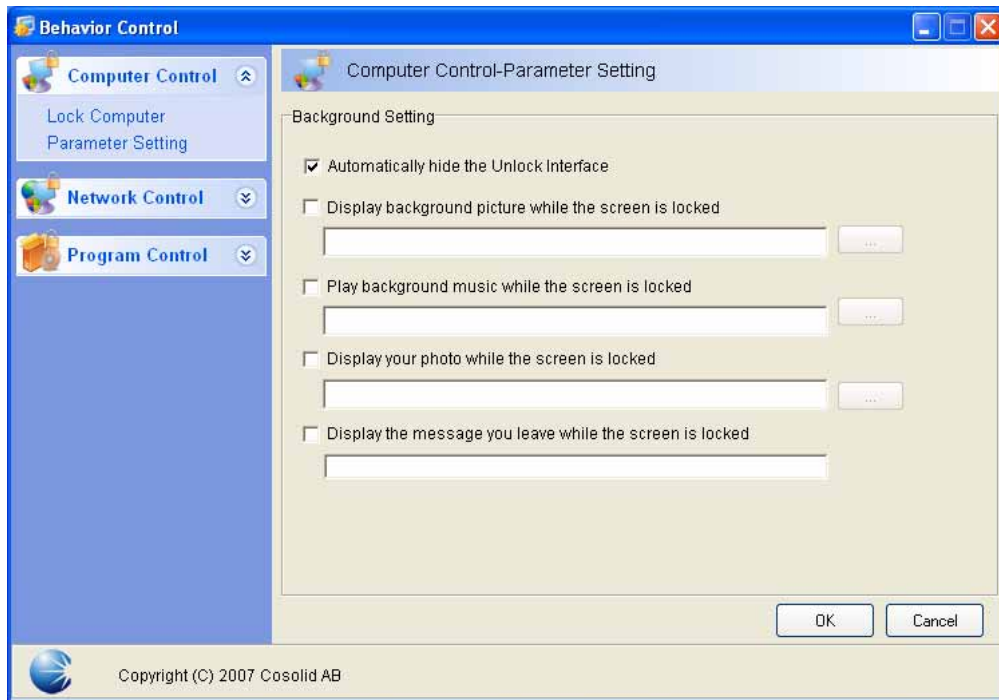
Prompt: *If the Subsection Time Control and Accumulative Time Control management are set at the same time, they will both effective. Rules are obeyed in the settings referred to the Subsection Time Control and Accumulative Control.*

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

Automatically lock the computer when waked up from stand by or hibernation state: At that time, if someone force to shut down the PC, restart it will result in automatic entering into the PC E-Lock Screen Saver.

4.3.1.3 Parameter Setting

Set the Background character of PC E-Lock Screen Saver which appear 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 locked computer, the system will automatically turn into the PC E-Lock Screen Saver. 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 image as the PC E-Lock Screen Saver Interface. To avoid pattern distortion, the user had better to choose the picture size according to your monitor resolution. We provided some delicate background patterns for download in our website, including 1024x768 and 800x600 image size. The system default is *“Disabled”*.

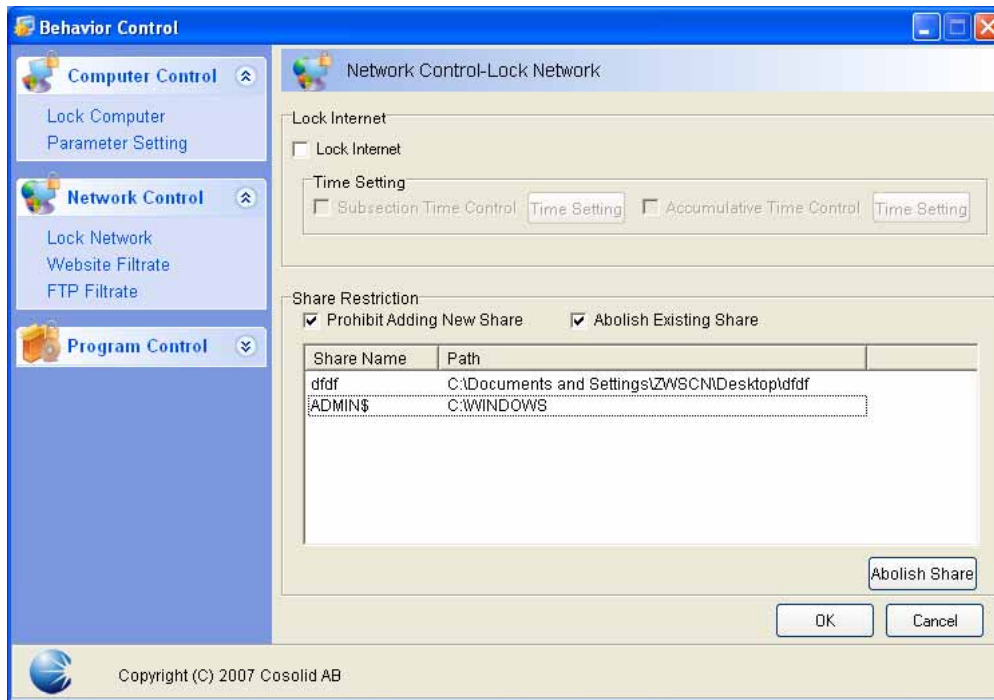
Play the background music while the screen is locked: When computer is locked, the system will play the background music with the PC E-Lock Screen Saver Interface appeared. Only”, mid” file of music is permitted. We provide some euphonic background music for download in our website. The system default is *“Disabled”*.

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

Display the message you left while the screen is locked: Roll screen display the message you left on the PC E-Lock Screen Saver 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 connecting computer with network under the controlled mode. Please refer as follows,



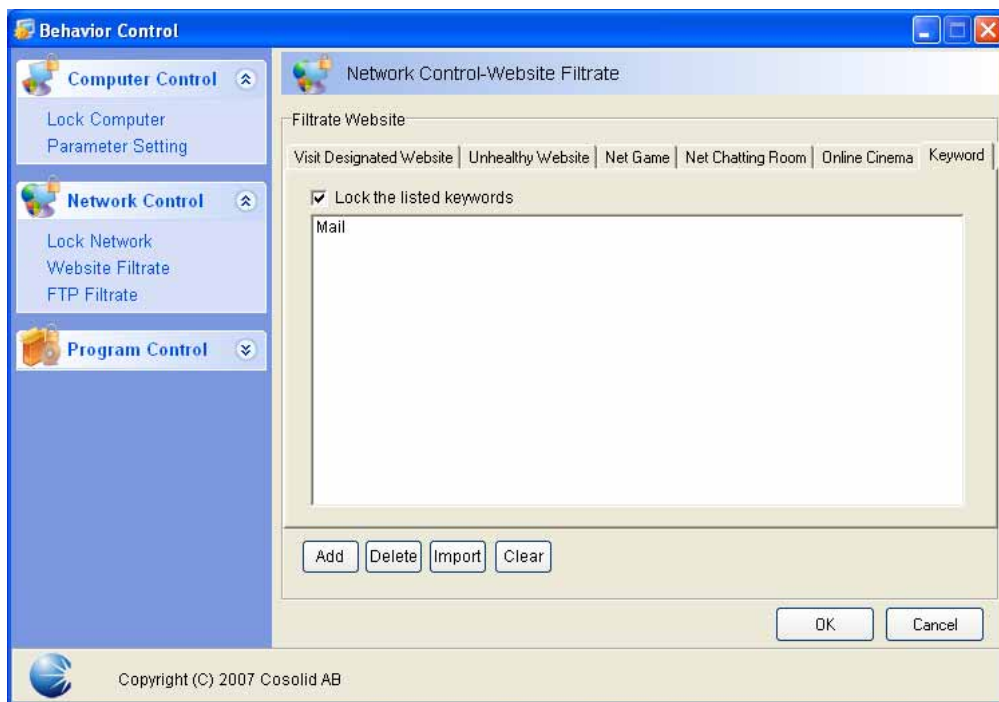
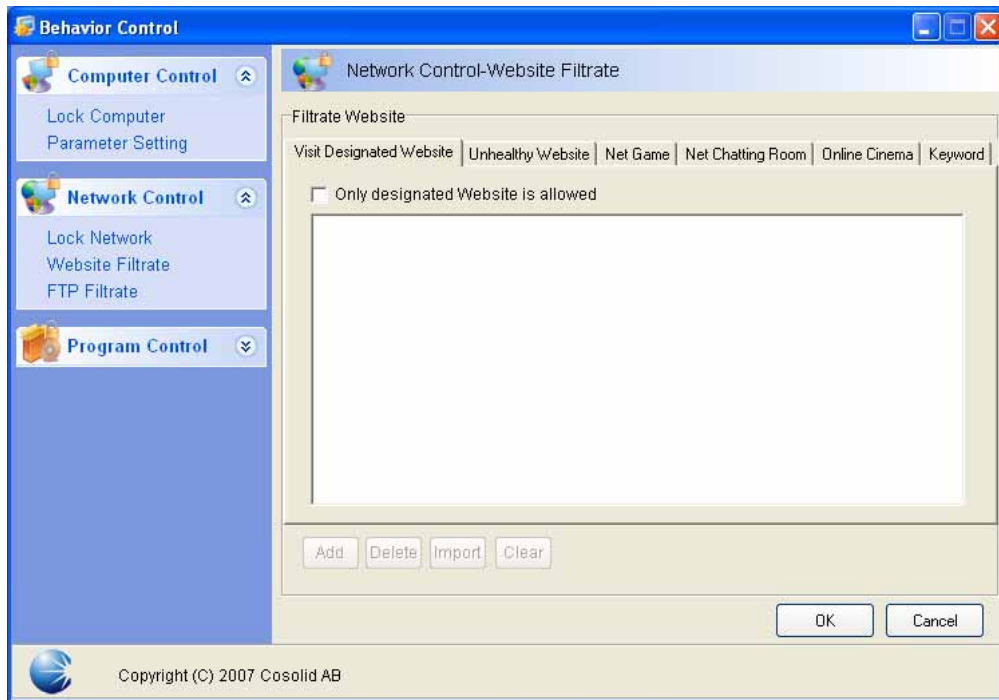
4.3.2.1 Lock Network

Provide functions of “*Lock Internet*” and “*Share Limitation*”. On the “*Lock Internet*”, you can “*Lock Internet*” according to your set Subsection and Accumulative Time Control setting. The system default is “*Disabled*” and “*Unlock*” all time, and the default accumulative time is 24 hours a day.

Provide “*Prohibit Adding New Share*” and “*Abolish Existent Share*” functions on the “*Share Limitation*”. Click “*Prohibit Adding New Share*” to forbid adding new share under the controlled mode. Contrarily, unclick it to permit adding. The system default is “*Enabled*”. Click “*Abolish Existed Share*” to abolish the current existent share from the share list. The operation steps are selecting the share item from list, and then clicking “*Abolish Share*” button. The “*Cancel Existed share*” function is efficient directly under the administrator mode. The function we designed is for users to direct operate all system shares and avoid possible forgetting because of too much shares effectively.

4.3.2.2 Filtrate Website

Provide functions of “*Visit Designated Website*”, “*Filtrate Unhealthy Website*”, “*Filtrate Net Game*”, “*Filtrate Net Chatting Room*”, “*Filtrate Online Cinema*” and “*Filtrate Keyword*”. Through website filtration, you can effectively control your visiting website character. Under the controlled mode, select “*Visit Designated Website*”, only the websites from designated website list can be visited; select “*Filtrate Unhealthy Website*”, “*Filtrate Net Game*”, “*Filtrate Net Chatting Room*”, and “*Filtrate Online Cinema*”, the system default is “*Locked the websites which are of the character from the PC E-Lock database and added to the filtrate website list*”; select “*Filtrate Keyword*” and the system default are “*Locked websites which are of the keyword character form the keyword list*” and to input three keywords - “*mail*” “*mailbox*” and “*E-mail*” (In that case, all websites which used to send E-mail are unable to open). The system default is Enabled “*Filtrate Unhealthy Website*” and “*Filtrate Keyword*”. Import the file as “*.txt*” with website or keyword, and one website address or keyword is for one line. Same website or keywords imported will not be repeated, as follows,

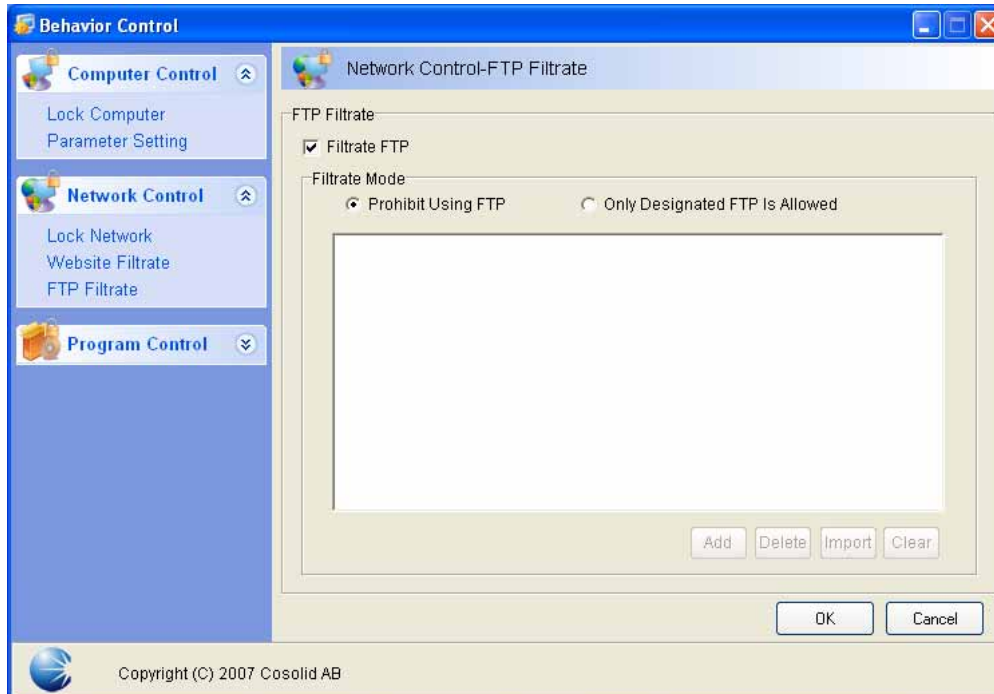


Prompt: Once “Lock Internet” selected, PC E-Lock Smart will lock all functions of network automatically. The chatting tools and relative programs with internet will be failure in connecting with internet.

Prompt: The adding website must be of the First Class Domain Name. Fox example. Both <http://www.cosolid.com> and <http://www.cosolid.com/index.htm> are the same Class Domain Name. You must type whole website address, namely, “http: //www.” not www.cosolid.com or cosolid.com. Then all websites including cosolid.com will be forbidden or designated.

4.3.2.3 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 the controlled mode. The system default is Enabled “*Prohibit using FTP*”. As follows:



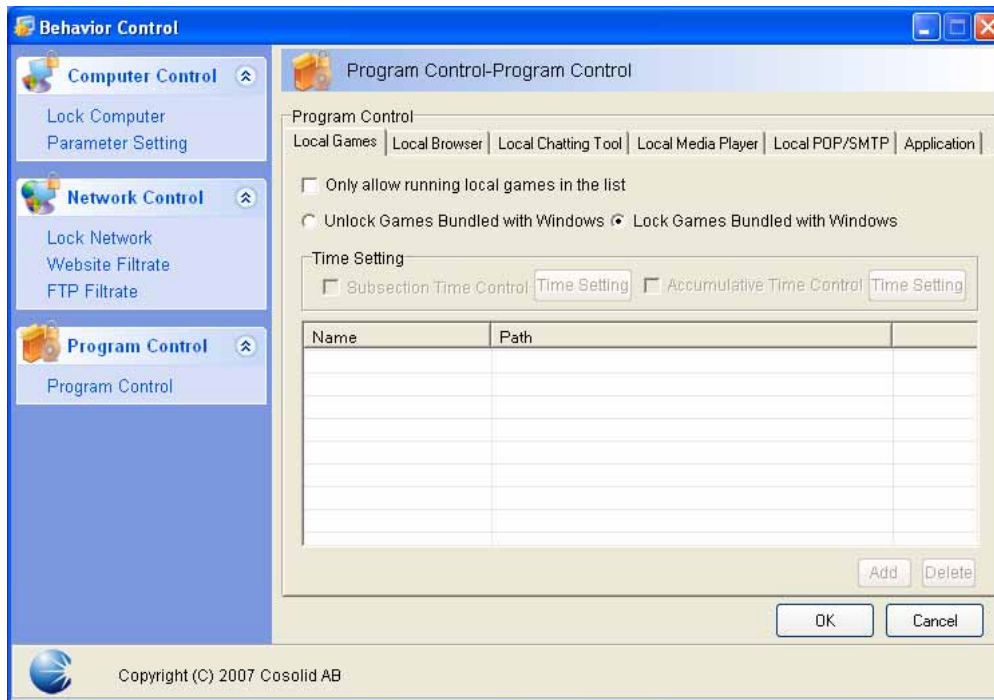
4.3.3 Program Control

Provide functions of “*Application Control*”, “*Local Games Control*”, “*Local IE Control*”, “*Local Chatting Tool Control*”, “*Local Media Player Control*”, “*Local POP/SMTP Control*”. You can effectively control the program (lock software of computer) under the controlled mode by “*Program control*”.

Note: Please select “*Subsection Time Control*” or “*Accumulative Time Control*” after unlock any module of the settings. Otherwise, all programs are remaining blocked as default.

4.3.3.1 Local Games Control

Select the function; you can set your allowing games. Provide “*Lock Games bundled with Windows*” and “*Unlock Games bundled with Windows*” functions. (Such design is that can meets the user’s requirement for limiting local games but running local games bundled with Windows.) “*Lock local games*” can be set according to your Subsection and Accumulative Time Control setting. The system default is “*Disabled*” and “*Unlock*” all time, and the accumulative time is 24 hour per day. As follows,



4.3.3.2 Local IE Control

Select the function and you can set your allowing browser. It can control IE according to your Subsection and Accumulative Time Control setting. The system default is “Disabled” and “Unlock” all the time, and the accumulative time is 24 hour per day.

4.3.3.3 Local Chatting Tool Control

Select the function and you can set your allowing local chatting tools. It can control the local chatting tool according to your Subsection and Accumulative Time Control setting. The system default is “Disabled” and “Unlock” all the time and the accumulative time is 24 hour a day.

4.3.3.4 Local Media Player Control

Select the function and you can set your allowing local media players. It can control the local media player according to your Subsection and Accumulative Time Control setting. The system default is “Disabled” and “Unlock” all the time, and the accumulative time is 24 hour a day.

4.3.4.5 Local POP/SMTP Control

Select the function and you can set your permitted local POP/SMTP. The system default is “Disabled”.

4.3.4.6 Applications Control

Set your allowing applications here. The default is enabling for 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. It can effectively control the software under the controlled mode.

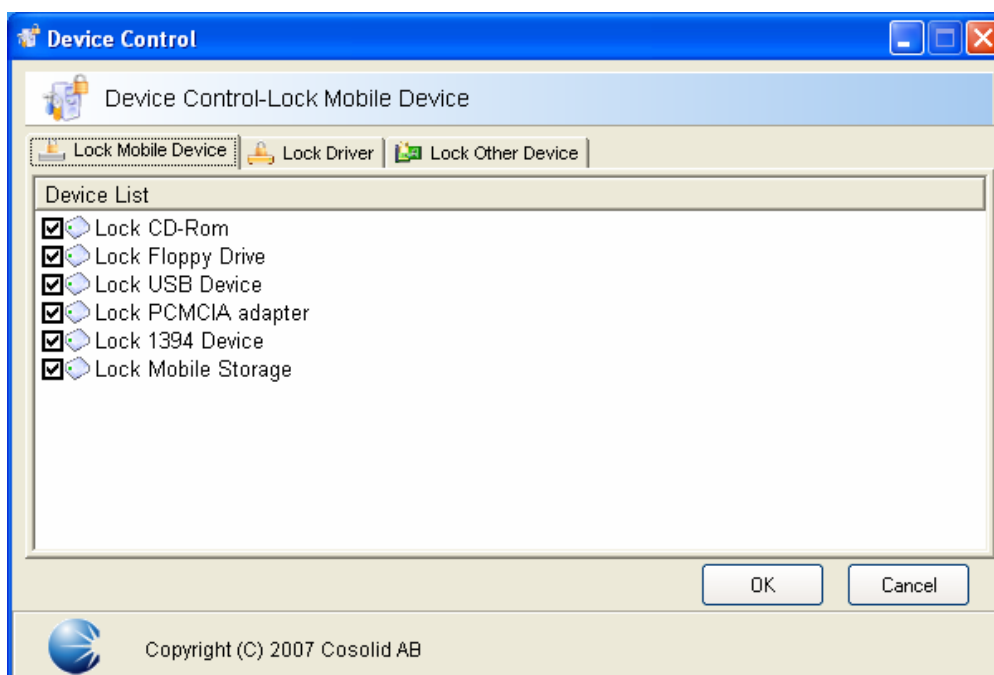
4.4 Equipment Control

Provide functions of “*Lock Mobile Device*”, “*Lock Drive*” and “*Lock Other Device*”. Through “*Equipment Control*” on computer (means to lock the hardware), you can effectively control the hardware using under the controlled mode. Select devices which you need to lock from hardware list provided then click “OK” to save.

Prompt: Adding shortcut of any program is effective.

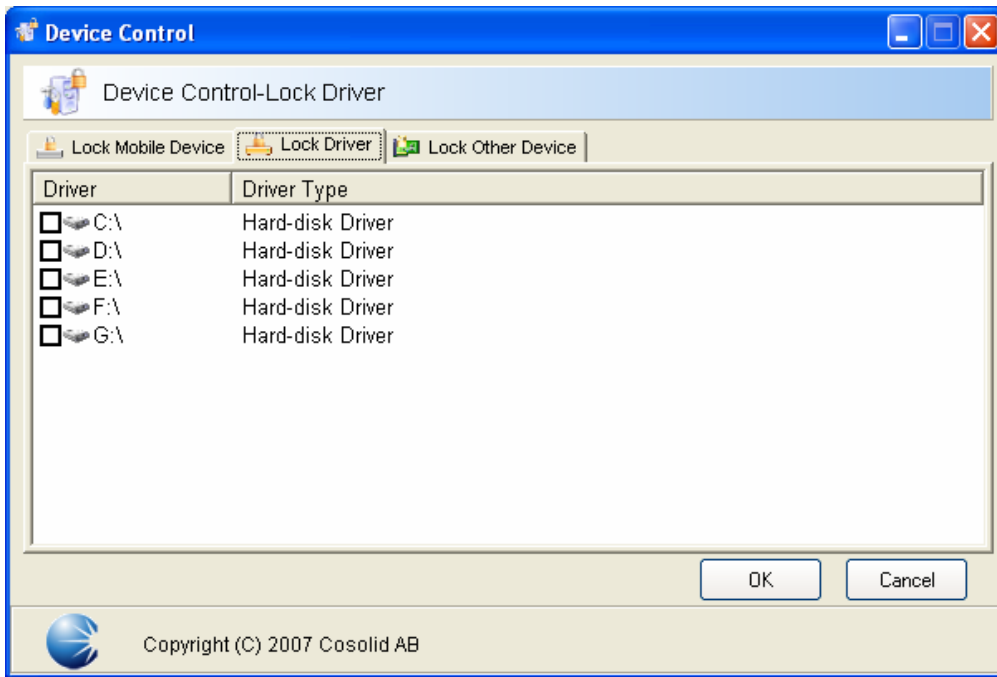
4.4.1 Lock Mobile Device

Provide “*Lock CD –Rom*”, “*Lock Floppy Drive*”, “*Lock USB Device*”, “*Lock PCMCIA Adapter*”, “*Lock 1394 Device*”, and “*Lock Mobile Storage*” etc. Here you can effectively control the computer to install or copy the adult, violent or unhealthy software, games, programs and files through the equipment and avoid virus, unhealthy intrusion and secret file revealed under the controlled mode. The system default is “*Lock all devices*”. As follows,



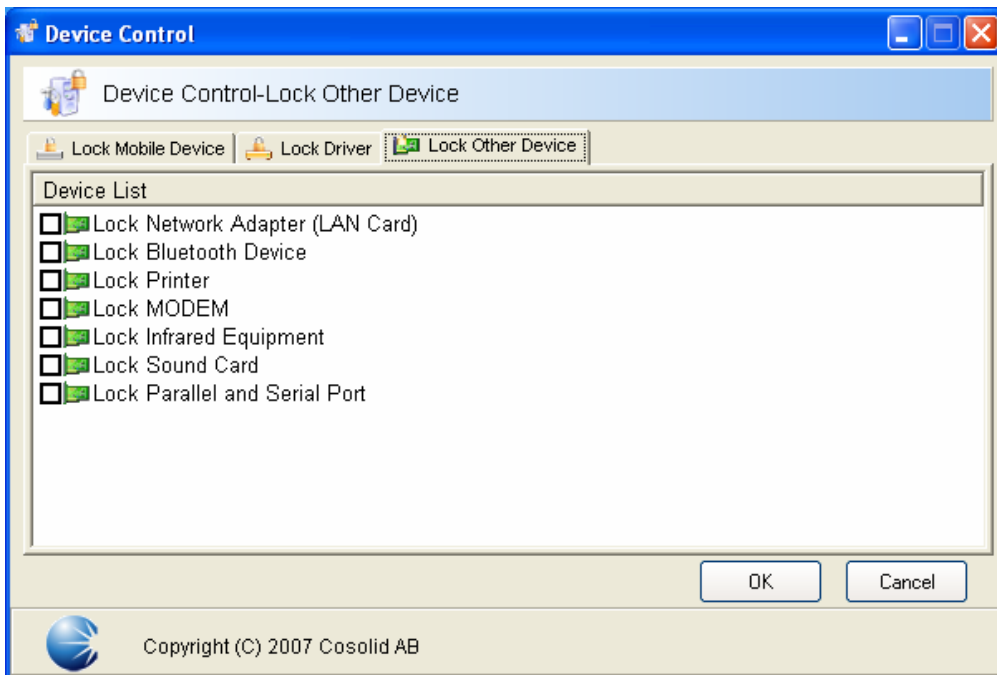
4.4.2 Lock Drive

Provide all current drivers list which contains drivers and extended drivers connected with PC for your lock selection. As follows,



4.4.3 Lock Other Device

Provide “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,



4.5 Data Security

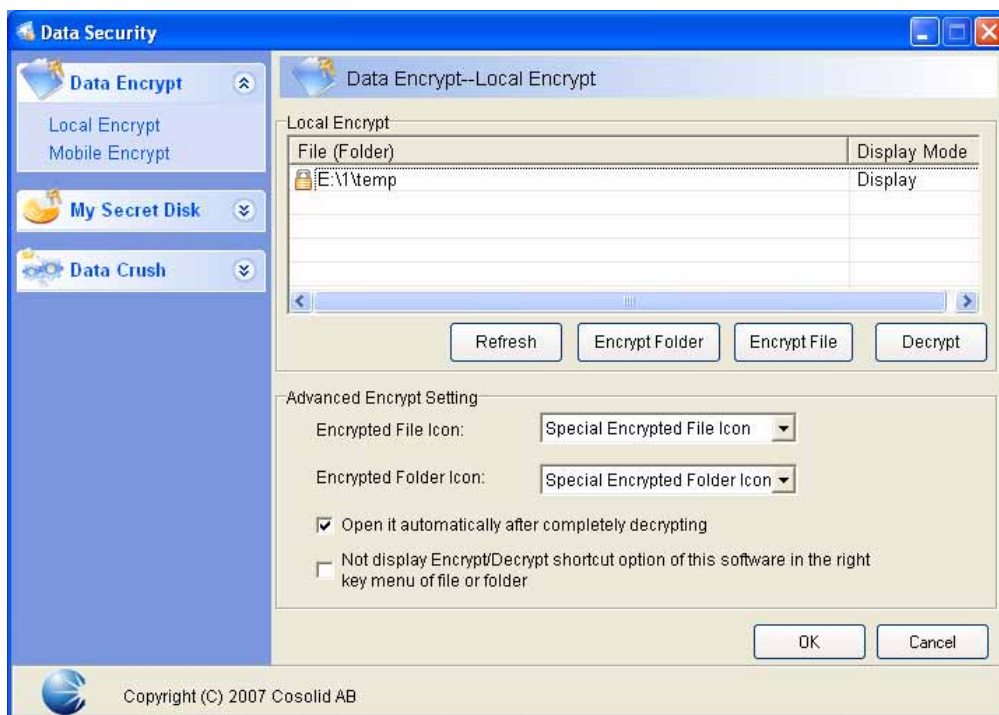
Provide functions of “Data Encrypted,” “My Secret Disk” and “Data Crush” By Data Security, the possibilities of revealing or modifying or deleting the secret data will be effectively controlled.

4.5.1 Data Encrypted

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

4.5.1.1 Local Encrypt: It is the highest security.

- File or folder which has been encrypted will be unable to open or decrypt, even if it is renamed or copied to other places.
- File or folder which has been encrypted can still be found and opened or decrypted from encrypted file (folder) list on the “Data Encrypted” Main Menu (see the below figure), even if it is deleted.
- If the encrypted file or folder is cut, you are unable to open or decrypt them in the new path, but can still find and open or decrypt from encrypted file (folder) list on the “Data Encrypted” Main Menu (see the above figure). It can effectively prevent others from using, deleting or modifying the storage path or modifying the storage path or copying your data in the computer.

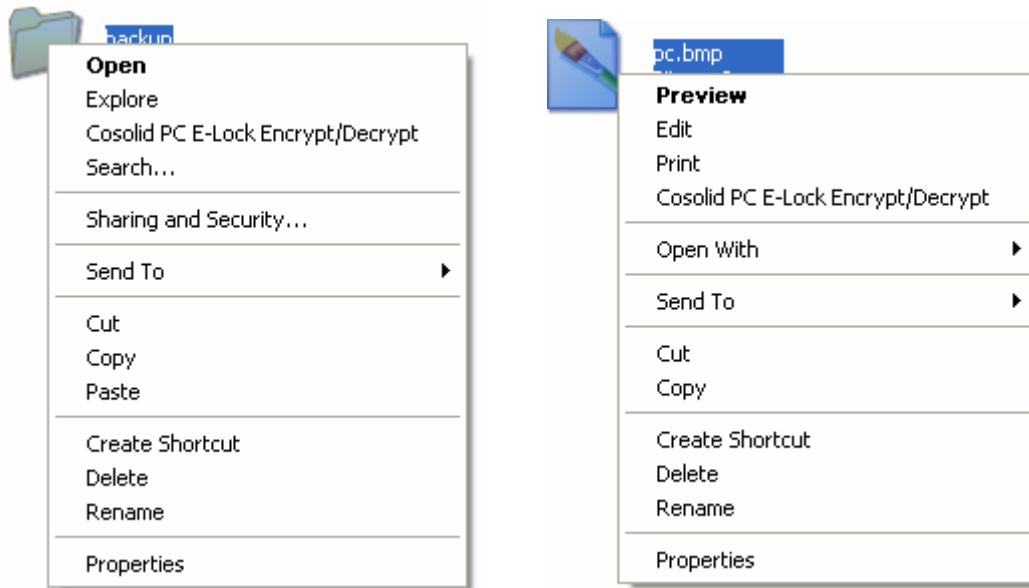


Prompt: No matter which equipment you select, we are setting to unlock any kinds of keyboard and mouse (USB, parallel and serial port or wireless).

- Copy your data in to the computer.

Provide an encrypted file (folder) list. You can add the file (folder) which you need to encrypt to the list by selecting “Encrypted File” or “Encrypted Folder”, displaying the file or folder path and encrypted way etc. 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. The file or folder will

be opened or decrypted. You are also able to encrypt or decrypt the file or folder by clicking “Encrypt” or “Decrypt” shortcut menu on the right- key of file or folder on 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 explorer. The system default is “*Display*”.



•Design some parameters as a matter of user convenience as follow,

Encrypted File Icon Display: Provide three different icons.

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

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



Note:

- Adopt “Hide” to display the file or folder by “Local Encrypt”. Since it cannot be found on the explorer, you must decrypt it on the “Data Encrypted” Main Menu (see the above figure).
- After reinstalled OS, all encrypted files or folders will keep encrypted state and original password all the same. You are able to decrypt them when re-install the product.
- The encrypted folder cannot be in the partition where you will re-install OS, otherwise it can be deleted when re-install.
- After uninstalled, the original encrypted folder is unable to decrypted, moreover keeps encrypted state all the same. You are able to decrypt them when re-install the product.

Encrypted Folder Icon Display: Provide three different icons.

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

The system default is “Encrypted Special File Icon”.



Will not display Encrypt/ Decrypt shortcut menu of this software in the right- key of file or folder: Prevent others from knowing what you used. The system default is “Display Encrypt/Decrypt shortcut menu”.

Decrypt Completely and then Open: The system will automatically open the file or folder after 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 if you need to move. It can ensure security of moving file and folder mostly. The file or folder is of the following characteristics:

- The encrypted package which has been encrypted by mobile encrypt is the file as “. EXE”. The file can be deleted, copied, moved to other path or other computers while keeping encrypted state.
- No matter how the encrypted packages by mobile encrypt is copied or moved, it is able to be open or decrypted without installing PC E-Lock smart.



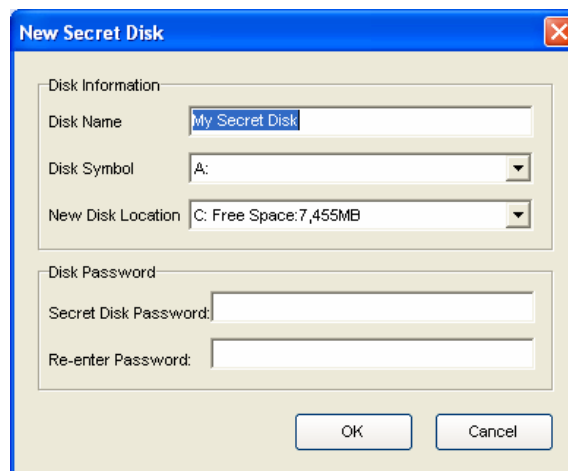
Click “Add File” or “Add Folder” to select the file or folder which you need mobile encryption (The file or folder path will display on the mobile encryption item). Select “Delete the original file or folder after mobile encrypted”. The system default is” Deleted”. Click “Mobile Encrypt” and input your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

Prompt: (Applied in Local Encrypt or Mobile Encrypt)

- The encrypted file is valid under safe mode and DOS or other operating systems.
- The encrypted function adopts the multiple encrypted methods which combine the exclusive developed encrypted technology with the current leading multiple encrypted technology. No matter who is proficient at computer or whichever tools are used, it cannot be decrypted. Therefore you must bear your password in mind.
- Please do not encrypt the folders which need to be used on the system folders such as "Windows", "Program Files", and "SYSTEM32" etc. Otherwise it is possible to cause the system error.
- The encrypted file or folder is not of copying and reading functions. So it can prevent the virus and Trojan from ruining and attacking.
- The encrypted file or folder is unable to execute, 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 not delete them. You can use the function to lock the file or folder with virus and then kill them after anti-virus software update.
- Data Encrypted support any program files like "EXE" etc.
- If the user locked a file or a folder, then a file or a folder shortcut will be ineffective.

4.5.2.1 New Secret Disk

Click "New Secret Disk", the system will appear the New Secret Disk Setting Interface. As follows,



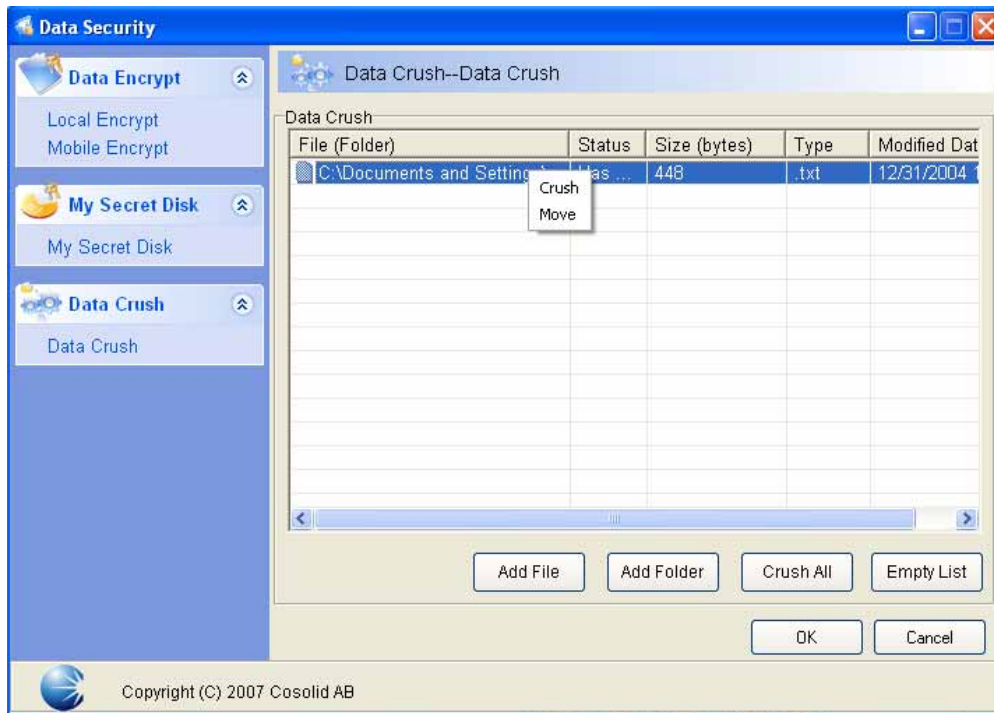
Set your new secret disk, including "Secret Disk Name" (support all different kinds of language naming, but these names does not exceed 16 Chinese characters or 32 characters, and the detailed stipulation is same as "WINDOWS partition naming", "Secret Disk Symbol", "New Space on" (means you select the 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". Click "OK" to display new secret disk item on the "Secret disk list". Provide secret disk list on "My Secret Disk" setting Interface, which lists all current secret disk items established (display Secret Disk Name, Secret Disk Icon, Main Disk, Used Space, Free Space etc.). Move the mouse to the secret disk item in the list and right-click, you can see the pull down menu then select the following options to operate the secret disk.

4.5.2.2 Open

Click “Open” and input your password. The secret disk explorer will automatically open the corresponding secret disk. You can operate them in the secret disk explorer, likely in the system explorer. You will find the secret disk icon on the OS explorer.

4.5.2.3 Close

Click “Close” or “✕” at the right-up corner of secret disk explorer to close the secret disk explorer.



Prompt:

- *The secret disk is that you set up one or more partition in original partition means it based on the original partition. We can consider it as “partition in partition”. The space of the original partition will reduce when adding files in the secret disk.*
- *After reinstall or uninstall this software, all the secret disk and data 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 cannot use the same name and disk icon, but can be set up on the same partition. All secret disks’ passwords may be different.*
- *After set up your secret disk, do not need to format .The partition is in the same format as the original partition.*

Important Statement: After deleted the secret disk in the secret disk explorer or in the system explorer, the data will not be 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”)

4.5.2.4 Delete

Click “Delete” and input your password to delete the disk.

4.5.2.5 Clear all Data

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

4.5.2.6 Secret Disk Setting

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

4.5.2.7 Import Data

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

4.5.2.8 Export all Data

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

Important Statement: After deleting the data in the secret disk, the data will be crushed and not 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”). The original used space will be released to the main disk, after deleting the “secret disk”

Important Statement: After emptying the secret disk, the data in these disks will not be 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”)

Prompt: Please confirm that 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 be fail!

4.5.2.9 Close all secret disks

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

4.5.3 Data Crush

Provide item list of the file (folder) which will 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) . 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 clear the file or folder item from the list. Click “Crush All” at the down corner of list to crush all files or folders. Click “Empty List” to delete all files or folders from the list. The crushed file or folder on the list will display “Crushed” as follows,

Database Encrypted:

- Backup the database files
- set up the private secret disk such as Z disk
- Reinstall administrator software and set up the install catalog or catalog default to the private secret disk such as Z disk

●When you do not login the PC E-Lock, the administrator software will prompt error, and the database are unable to be open. It is possible to use the software normally and open the database when you login the PC E-Lock.

Data Advanced Encrypted:

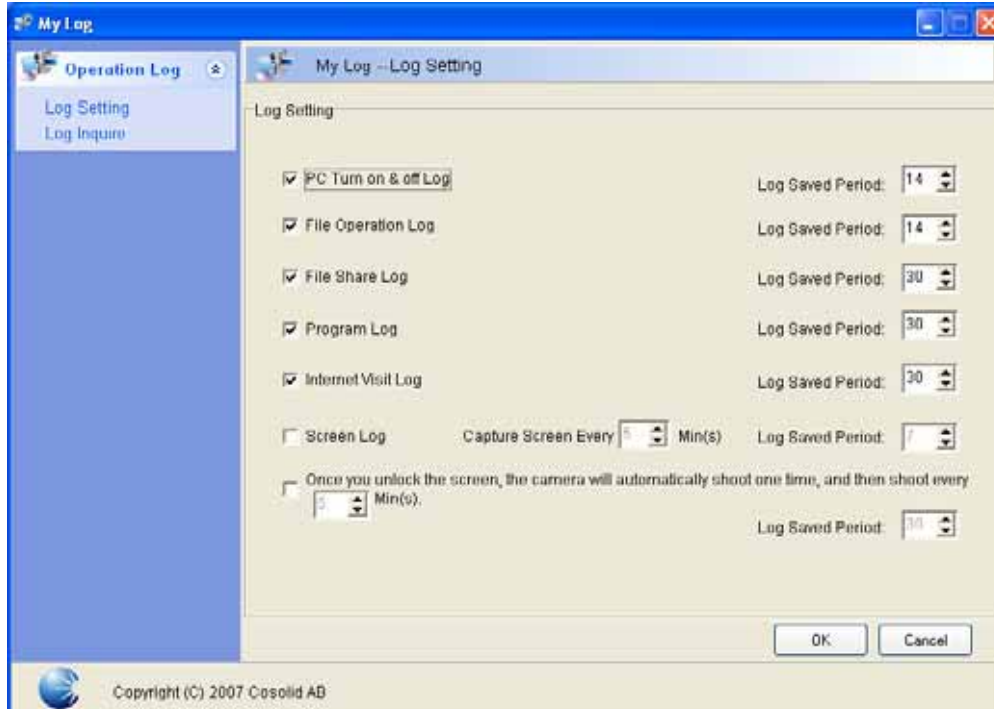
- Use mobile encryption to transfer
- Save data to my secret disk
- Encrypt the data file
- Encrypt the catalog where data file is again
- If so, your data has multi-protections. No one can guess your password easily and even decode. Certainly you can also use the compressible software such as WINRAR etc to encrypt compressible again.

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 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 scientific and rationality of PC E-Lock management setting under the controlled mode.

4.6.1 Log Setting

Set the time of saving Monitor Log. As follows:



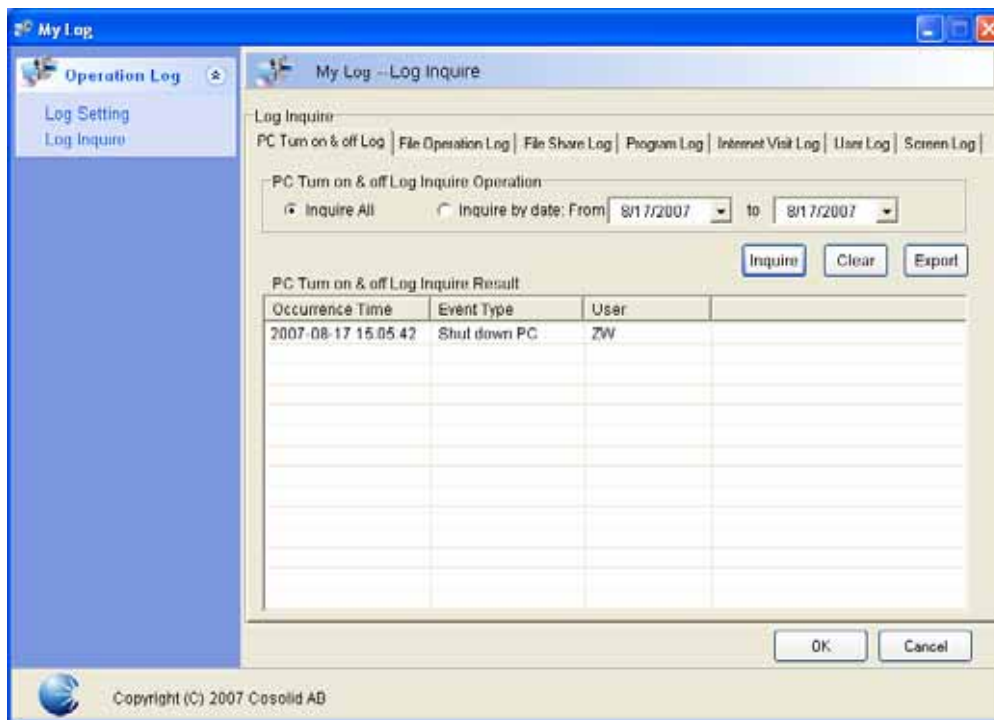
Important Statement: Data Crush function can not only be used to delete the file and folder, but also clear up the file and folder's information on the sector thoroughly. The crushed file or folder can't recover, even using the final data tool. Any behaviors trying to find out and restore the lost information will fail, so you should watch your step when execute the function.

4.6.2 Log Inquire

Provide "Inquire", "Clear" and "Export" Monitor Log stored Record according to the schedule. Press "Inquire" button to refresh the record in the current list. Click "Stop" button to stop tidying up the record. Click "Clear" button to clear up the current record. Click "Export" button to export the record into ".txt" file.

4.6.3 Start PC Log

Inquire conveniently about the details under the controlled mode, including PC Start, logout and turn off 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

Inquire conveniently about the details of file operation under the controlled mode, including Occur 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

Inquire conveniently about the details of file or folder share under the controlled mode, including Occur Time, User Name 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 Monitor Log

Inquire conveniently about the details of program running under the controlled mode, including Occur 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 Website Monitor Log

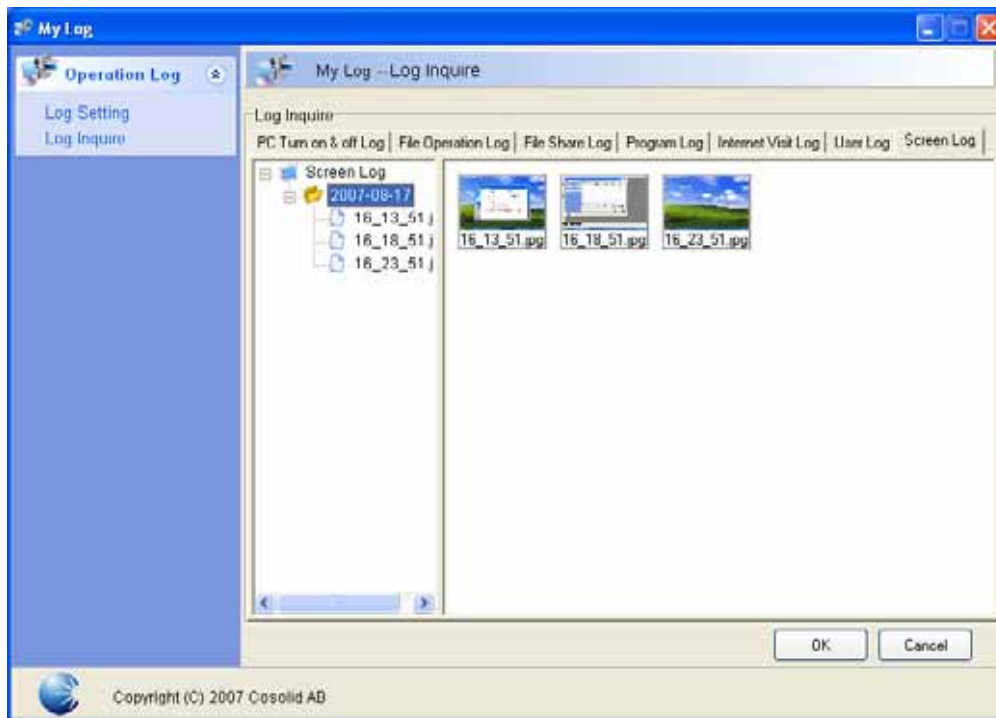
Inquire conveniently about the details of internet visiting under the controlled mode, including Occur Time, Website and Type etc. It can save the record for 0-30 days. The system default is 30 days and “Enabled”.

4.6.8 User Monitor Log

Inquire conveniently the user’s picture captured by the system in detail under the controlled mode. If someone uses your computer or input the locked password to enter into your computer when leaving, the webcam will automatically photo every other 5-60 minute, and the system default is 5 minutes. It can save the record for 0-30 days. The system default is 30 days and “Disabled”. Since the user’s photos need for large MD space, it is recommended to delete photos by pressing “Clear” button after you checking every time.

4.6.9 Screen Monitor Log

Inquire conveniently about the screen image under the controlled mode. Saving the screen image can be set every other 5-60 minute, with the system default 5 minutes; and the record can be saved for 0-7 days with the system default 7 days and “Disabled”. Since that the screen records need for large MD space, it is recommended to delete records by pressing “Clear” button after you checking every time. As follows,

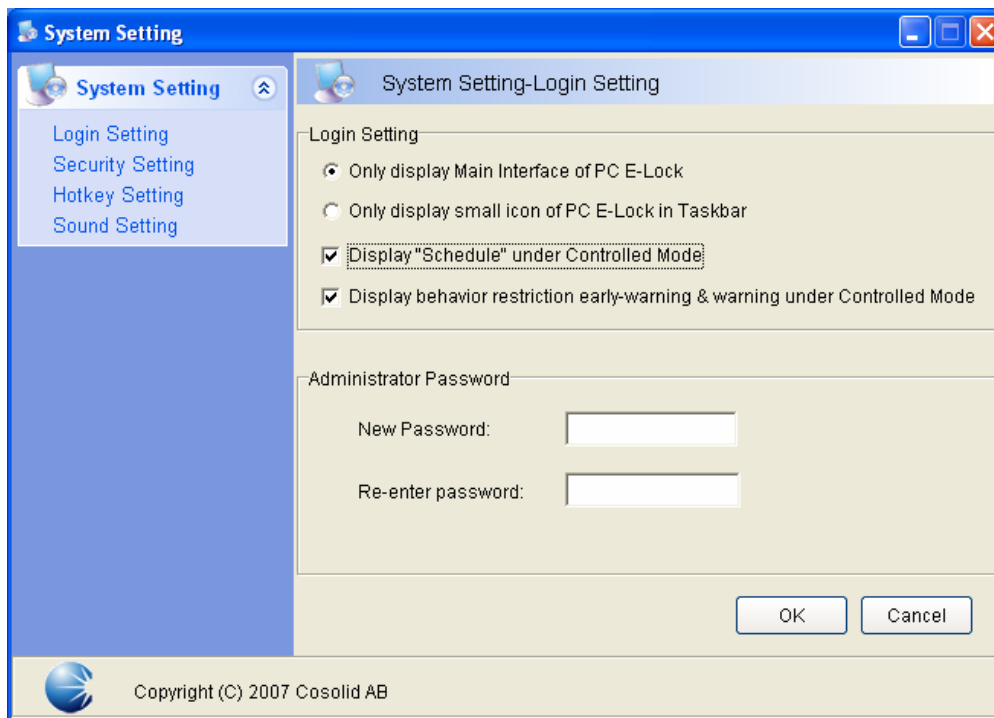


Prompt: For “user monitor log, install the webcam previously and adjust it to your face in your usual habit. Pleas adjust focus in order to capture your face clearly!

4.7 System Setting

4.7.1 Login Setting

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



4.7.1.1 The Main Interface of PC E-Lock

Only the Main Menu is displayed after login the product. The system default is *“Enabled”*.

4.7.1.2 The Small Icon of PC E-Lock Taskbar

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

4.7.1.3 under the controlled mode, show time tray

Under the control mode, the time tray will be displayed at the right-up corner of the screen. Once the user moves the mouse to the right-top of the screen, the time tray would appear. By contraries it would automatically hides. This facilitates you to view the computer behavior control schedule. All behavior control related to time will be displayed. The system default is *“Enabled”*.

Schedule	
Lock PC	Unlock
Eyes Protection	00:39:39
Lock Internet	Unlock
Lock Browser	Lock
Lock Games	Lock
Lock Chatting Tools	Lock
Lock Media Player	Lock
Lock POP/SMTP	Lock
Lock Program	Lock

4.7.1.4 Display time arrival prompt and limit warning under the controlled mode

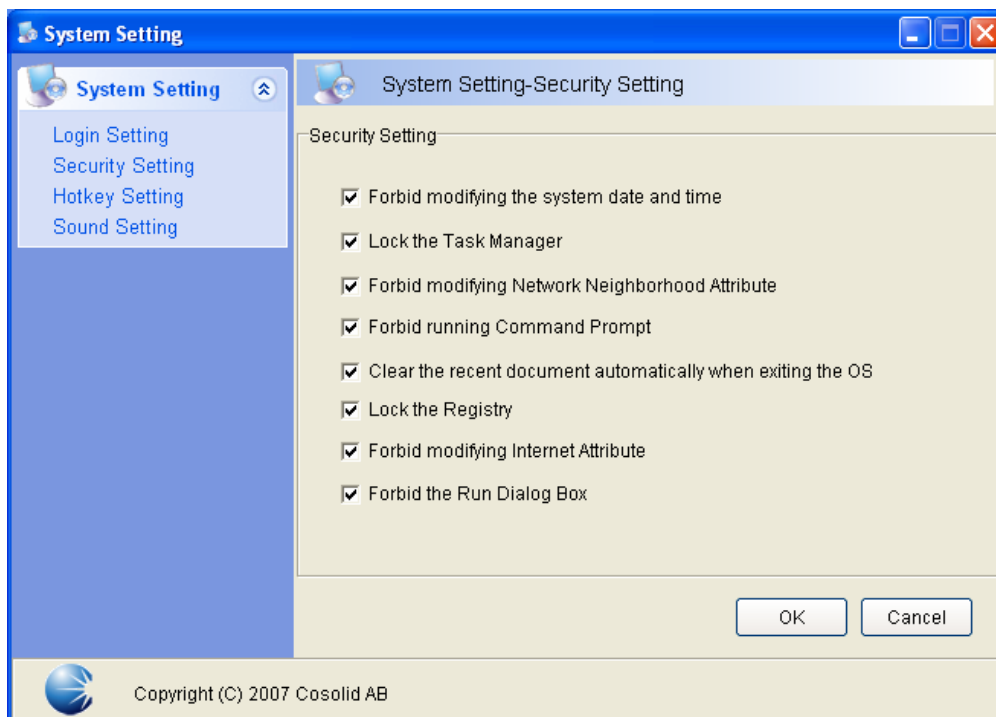
Under the control mode, time arrival prompt and behavior limit warning prompt will be displayed in the middle of the screen. For example, the system automatically popup the prompt in 5 minutes before game time arrives, under the control mode. In that case, enough time is considered for saving game and the management will be more humanized. Time arrival prompt is set for 5 minutes except eyesight protected mode for 1 minute and. The system default is "Enabled".

4.7.1.5 Administrator password

Modify the administrator password, which will be input directly into the lock.

4. 7.2 Security Setting

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



4.7.2.1 Forbid Modifying the System Date and Time

Forbid modifying the system time and date under the controlled mode. The system default is "Enabled".

4.7.2.2 Lock the Registry

Forbid opening the system registry under the controlled mode. The system default is "Enabled".

4.7.2.3 Lock the Taskbar Manager

Forbid opening the task manager under the controlled mode. The system default is "Enabled".

4.7.2.4 Forbid Modifying Internet Properties

Forbid modifying the system Internet properties under the controlled mode. The system default is "Enabled".

4.7.2.5 Forbid Modifying My Network Place Properties

Forbid modifying the My Network Place Properties under the controlled mode. The system default is "Enabled".

4.7.2.6 Taboo Running Dialog

Prompt: Strongly recommend set up BIOS password to prevent BIOS time from modification.

Taboo running the system dialog box under the control mode. The system default is "Enabled".

4.7.2.7 Forbid Running Command Prompt

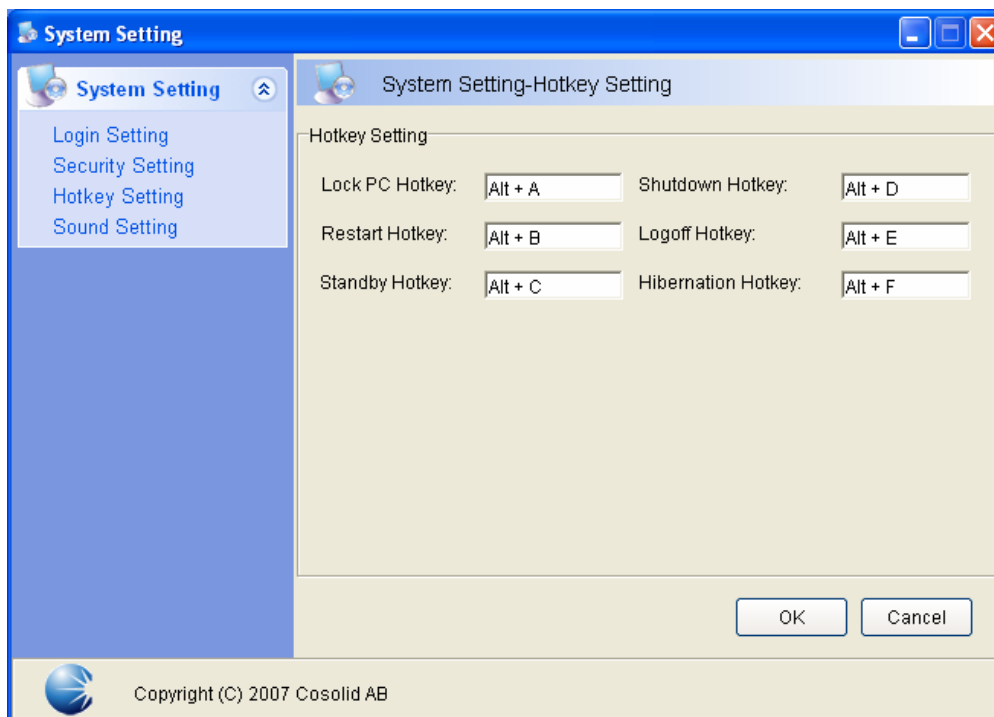
Forbid running the system command prompt under the control mode. The system default is "Enabled".

4.7.2.8 Exit the OS, and then clear the lately document automatically

Clear the documents automatically when switching administrator mode to control mode. The system default is "Enabled".

4.7.3 Hot-key Setting

Set up shortcut Hotkey for system control, for the convenience of your operation. As follows:



4.7.3.1 Lock PC Hotkey

Under the administrator mode, your computer can be locked directly by this hotkey unless the administrator unlock. To set up hot key, press the one which you want to set up into this hotkey box. (If the hotkey has been set up to control other program, the setting will be forbidden)

4.7.3.2 Shutdown PC Hotkey

Under the administrator mode, press this hotkey to turn off your computer directly.

4.7.3.3 Restart PC Hotkey

Under the administrator mode, press this hotkey to restart your computer directly.

4.7.3.4 Logoff PC Hotkey

Under the administrator mode, press this hotkey to log out your computer directly.

4.7.3.5 PC Standby Hotkey

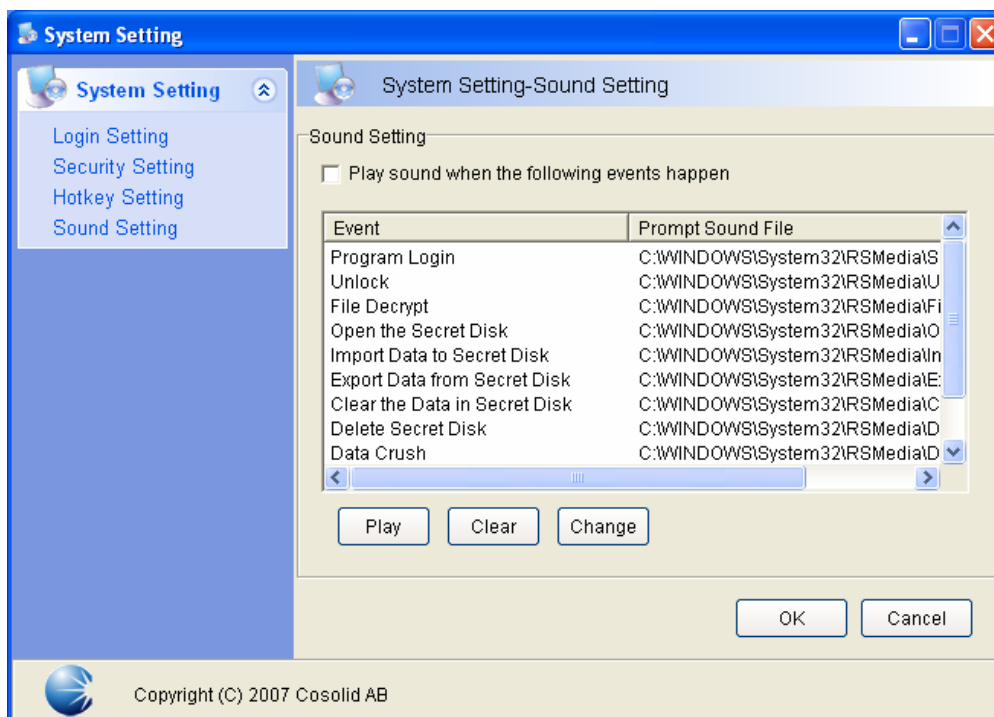
Under the administrator mode, press this hotkey to make your computer standby directly.

4.7.3.6 PC Hibernation Hotkey

Under the administrator mode, press this hotkey to make your computer hibernate.

4.7.4 Sound Setting

Set the sound prompt when some events of PC E-Lock happen (including “*Program Loading*”, “*Unlock PC*”, “*Decode 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 can only be “wav” format. The system provided the sound default for these events.



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

4.7.4.1 Play

Select the event of which you want to pre-hear the sound 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 Browse

Select the event of which you want to change the sound from the event list, and then click “Browse”; you can choose the sound which you like for the event.

Chapter 5 FAQ

6.1 Does PC E-Lock affect other software running after the game and internet locked?

A: It will not affect other software running except some special 2D/3D graph and image processing program.

6.2 Is there 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 little functions but with following shortcomings:

- Easy to decoded.
- Easy to uninstalled and deleted by administrator.
- Easy to terminated and deleted program in the registry and task manager.
- Invalid under in safe mode.

Please be cautious to purchase.

6.3 Can the function of lock unhealthy website block the healthy?

A: It is possible. It is rather difficult to confine the unhealthy information. The information unhealthy or specified to the adult actually exists in the webpage which contains the keywords like "*Female*", "*life*" and "*Make friends*". The product adopts the strict measure to extremely block the adult topic display, together with possible affection to browse news webpage. Regard of this, parent and administrator should see both side of it.

6.4 Update

We provide two ways to update the product:

- Click "*Update*" option on the right key menu of small icon on taskbar, system will automatically prompt that update package is found and now it is updating (subject to update package verse NO. and date). There is no need to uninstall the old version's software when update.
- Old version can not be updated to this version V9.0 since the hardware is different.