

In the Name of God

Arg

User Manual

Version 1.2



PayamPardaz Engineering Company

May 2014

Table of Contents

Subject	Page
1 Introduction	1
2 Software Terminology	2
3 Install	4
4 Run	4
5 Login	5
6 Software Initial Configuration	6
6.1 Change PIN	6
6.2 Change Master PIN in KeyA2 Token or <i>PUK</i> in KeyA3 Token	7
6.3 Create New Profile	8
6.4 Create a Secure Partition	9
7 Software Settings	13
7.1 General Settings	13
7.2 Virtual partition Settings	14
7.3 Mount Settings	15
7.4 Log Settings	15
8 PIN Management in KeyA Token	16
8.1 Change KeyA Token PIN	17
8.2 Change KeyA3 Token Admin PIN	17

8.3	Change KeyA2 Token Master PIN or KeyA3 Token <i>PUK</i>	17
8.4	Define Token PIN.....	18
9	Profiles Management.....	18
9.1	Modify Profiles.....	18
9.2	Import Profiles from Backup File to Token	20
9.3	Upgrade From Hoda Software to <i>Arg</i> Software	21
10	Create Secure Virtual Partition.....	22
11	Pin Virtual Partition on Dashboard	24
12	Mount Secure Partition.....	25
13	Partitions Automatic Mount	26
14	Change a Partition's Properties	27
15	Protect Secure Virtual Partition Image File.....	28
16	Dismount Partitions	29
17	Unpin Partitions from Dashboard.....	29
18	Share secure virtual Partitions	29
19	Tools	30
19.1	Create backup from header.....	30
19.2	Restore header	30
20	Exit	31
1	Introduction	1
2	Software Terminology.....	2
3	Install	4
4	Run	4
5	Login	5
6	Software Initial Configuration.....	6
6.1	Change PIN	6
6.2	Change Master PIN in KeyA2 Token or <i>PUK</i> in KeyA3 Token	7
6.3	Create New Profile	8

6.4	Create a Secure Partition	9
7	Software Settings.....	13
7.1	General Settings.....	13
7.2	Virtual partition Settings	14
7.3	Mount Settings.....	15
7.4	Log Settings.....	15
8	PIN Management in KeyA Token.....	16
8.1	Change KeyA Token PIN.....	17
8.2	Change Keya3 Token Admin PIN.....	17
8.3	Change KeyA2 Token Master PIN or KeyA3 Token <i>PUK</i>	17
8.4	Define Token PIN.....	18
9	Profiles Management.....	18
9.1	Modify Profiles.....	18
9.2	Import Profiles from Backup File to Token	20
9.3	Upgrade From Hoda Software to <i>Arg</i> Software	21
10	Create Secure Virtual Partition.....	22
11	Pin Virtual Partition on Dashboard	24
12	Mount Secure Partition.....	25
13	Partitions Automatic Mount	26
14	Change a Partition's Properties	27
15	Protect Secure Virtual Partition Image File.....	28
16	Dismount Partitions	29
17	Unpin Partitions from Dashboard.....	29
18	Share secure virtual Partitions	29
19	Tools.....	30
19.1	Create backup from header.....	30
19.2	Restore header	30
20	Exit	31



1 Introduction

Data storage tools such as hard disks, flashes, and other portable disks contain electronic information about individuals and organizations. Since unauthorized access to this storage tools is probable through direct access, access through network, and theft; the possibility of sensitive and confidential information always threatens individuals and organizations. Therefore secure storage of sensitive and valuable data is an important need of today's *IT* world.

The disc encryption software, *Arg*, is a product to store data on different drives of computer such as a hard disk, *USB* flashes and other portable disks in a secure way. In this software one or several secure virtual partitions are created in computer whose all inner files and folders are encrypted. User or application accessibility to these partitions is completely transparent. In fact, *Arg* software encrypts data while they are being written on secure partitions and decrypts them while reading. All of the actions happen automatically and with no need to user involvement. The encrypted data are temporary in *RAM* and as a result no access to secure partitions information would be possible for unauthorized individuals.

The program uses an *Image File* (encrypted) to store secure virtual partition information. In this way after mounting, the image file will be mapped to an accessible virtual drive.

Arg software uses a key for disks encrypting operations. This key is stored securely in a hardware token named *KeyA* (*W*, *NW* and *T* models). Since working with *KeyA* security token needs a *PIN*¹, the accessibility to secure partitions is controlled in a two-factor way. In fact neither the accessibility of an unauthorized individual to another individual's token can threaten the security of a secure partition.

Arg software enables you to define several different profiles to immunize disks. The user specifies a profile while creating a secure partition, but at the time of the secure partition being used, the used profile is achieved automatically. Users can share their secure partitions among each other in case of agreement on some of the profiles.

Specifications of *Arg* software are as follows:

Creating secure virtual partition on hard disk as *Image File*

The ability to automatically *Mount Image File*

The possibility for one or several users to access *Image File* as read only

The use of exclusive password algorithm to encode data that can be ordered by customer

¹ *Personal Identification Number*



Access to secure drives by the use of *KeyA* token and the related personal ID

Store profile on *KeyA* token in a completely secure way

The ability to define several different profiles to immunize disks

The possibility that enables administrator to prevent user from changing profile

The transparency of secure partitions from user and application point of view

The possibility of creating a backup from partition header as an external file in order to recover secure partition data

Automatically creating backup from partition header internally

Temporary decrypting secure partition information in *RAM* memory

The ability to mount *Image File* from portable disks like *USB* flashes, *CDs* and *DVDs*

The ability to transfer *Image File* to other computers

The possibility of creating *Image File* with dynamic capacity

The possibility of rapid partition format

Filling free spaces of secure partition with random bits when no time pressure exists

Impossibility of observing the secure partition details such as file names, folder names, their contents and disk's free spaces for unauthorized users

2 Software Terminology

In this part we explain about words and expressions used in *Arg* software.

User: is the user of software. User needs a correct *KeyA* token to use software. A correct *KeyA* token is a *KeyA* token of *W*, *NW* or *T* model that is specifically locked by software vendor.

Secure virtual partition: is a secure drive whose internal contents are encrypted in a way that unauthorized individuals cannot read or use it. This drive is created virtually on computer by *Arg* software. The partition's information will be stored to an *Image File*. At the use time, the contents of *Image File* will be mapped to a virtual partition.

Token: is a hardware that saves profiles that the software uses for encrypting and also decrypting data in a completely secure way.

Profile: any encryption operation needs a key which is considered to be a string of 0 and 1 bits. The security of an encrypting system completely depends on key, therefore most attempts must be done to keep it and prevent it from being predicted. In *Arg* software, a key with its name is called profile. Profile key is a *Hexadecimal number*, this means that only characters of 0 to 9 and *a* to *f* can be received. The length of this key is 256/128 bits which is shown with



64/32 characters in *Hexadecimal* and are stored completely secure in KeyA token.

Mount: to work with a secure partition first the *Image File* must be mounted by *Arg* software. In this mode the mounted partition can be recognized as a general drive in windows.

Dismount: to inactivate a secure partition, it must be dismounted.

PIN: PIN is related to activating a KeyA token. By this password you may login *Arg* program and use its facilities. The default value for PIN of KeyA2 token is *keya* word and for KeyA3 token is *usr1*. Of course, for security matters, it is strictly recommended that user change the default value at the beginning of the work.

Master PIN (specific for KeyA2 tokens): each KeyA token has a Master PIN .

Besides, the general user PIN. The person who accesses the Master PIN can lock the profile in the token and prevent it to be changed by user. . Besides, anybody who accesses *Master PIN* may change PIN of the user without knowing what the previous PIN is. The default value for *Master PIN* of KeyA2 token is *keya*. For security matters, it is strictly recommended that user change the default value at the beginning of the work.

Role (specific for KeyA3 tokens): there are two types of users defined in KeyA3 tokens that are general user and administrator user. General user may login program and use its facilities or define a profile, delete or edit it. Administrator user may only lock profiles and prevent them from being changed by general user but he/she cannot login system with his/her PIN (*Admin PIN*).

Admin PIN (specific for KeyA3 tokens): is a password specific for administrator user to lock or unlock a profile. It is impossible to login program by this password. The default value of KeyA3 tokens *Admin PIN* is *adm1* word. Of course, for security matters, it is strictly recommended that user change the default value at the beginning of the work.

PUK (PIN Unlock Key: specific for KeyA3 tokens): each KeyA3 token has a PUK besides PIN and Admin PIN. Anybody who accesses *PUK* of a KeyA token may change PIN of the user (general or administrator) without knowing what the previous PIN is. The default value for *PUK* of KeyA3 token is *keya3*. For security matters, it is strictly recommended that user change the default value at the beginning of the work.

Administrator: is a person who has Master PIN in KeyA2 tokens or *Admin PIN* in KeyA3 tokens and is able to prevent profiles from being changed by users.



Software Dashboard: is the software environment that contains mounted or pinned partitions (Figure 1).

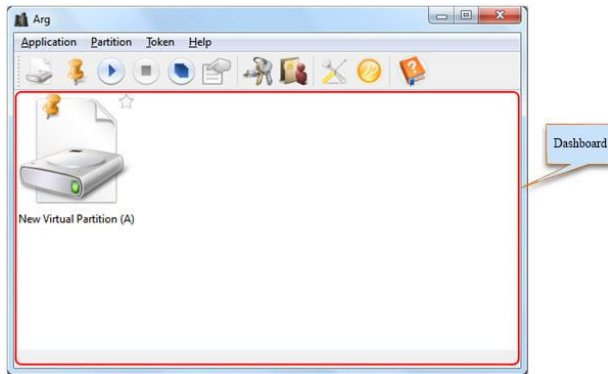


Figure 1- The main Window of Arg software

3 Install

To install *Arg* software, run *Setup.exe* program from product CD and then follow install steps. When install operation is finished, *Arg* software folder will be created in the specified location, in which an executive program named *Arg.exe* will be located. Moreover a shortcut named *Arg* in *Start Menu / All Programs / ARG* and one on computer desktop will be created.


Note: the user who installs the software must have an account of *Administrators* group on computer.

4 Run

To run *Arg* software, use the existing shortcut on computer desktop, or type *ARG* command in *Menu / All Programs* path from Start menu of windows; or run the *Arg.exe* executable file in software install folder.

Note: while running software in *Vista* or *7* windows environments, an alarm message of *User Account Control* related to run in *Administrator* mode will appear. Click *Allow* button in this window.



By running software, the program icon formed  will be appeared in *Tray Icons* part in the right side of Windows taskbar. By right clicking on this icon, a menu will appear that offers user program facilities (Figure 2).

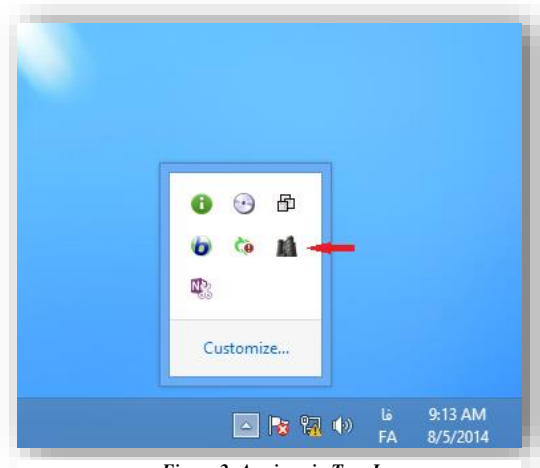



Figure 2- Arg icon in Tray Icons

5 Login

To use Arg software and access its facilities, first login to it according to these steps:

1. Attach correct KeyA token to computer *USB* port.
2. Run the program by clicking on its icon then the software login window (Figure 3) will appear.
3. Enter your PIN and click on  button.

Warning: user must note that ten times of sequential entering wrong PIN causes the token to be locked. In this mode, administrator can redefine a PIN by Master PIN (in KeyA2 tokens) or *PUK* (in KeyA3 tokens).

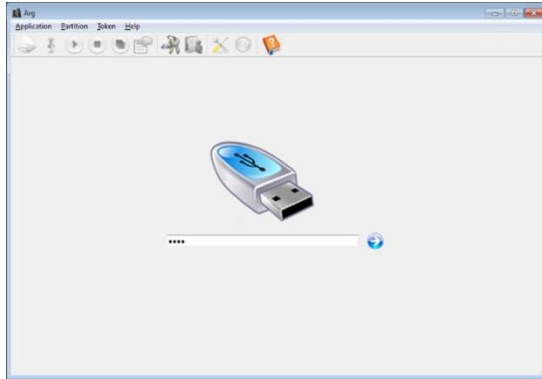


Figure 3-Arg login window

6 Software Initial Configuration

If you are running program for the first time after installation, a wizard window guides you to apply Initial settings to use program. The program configuration steps are as follows:

6.1 Change PIN

In this step you must enter a string of numbers and characters. Note that you cannot continue unless new PIN has been entered (Figure 4).

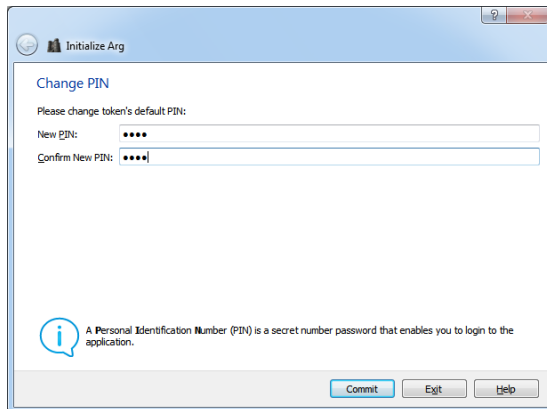


Figure 4- Change PIN



6.2 Change Master PIN in KeyA2 Token or *PUK* in KeyA3 Token

In this stage you must enter a new Master PIN for your KeyA2 Token or a new *PUK* for your KeyA3 token which contains numbers and characters. From security point of view, you'd better enter a different Master PIN or *PUK* from PIN. Note that you cannot continue the operation unless the new administrator Master PIN (or *PUK*) confirmation has been entered (Figure 5 and Figure 6).

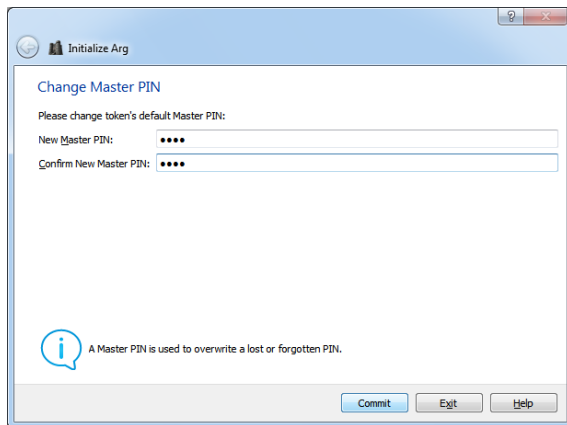


Figure 5- Change Master PIN (KeyA2 token)

Warning: it is strictly recommended that the default value of PIN and Master PIN or *PUK* be changed. Otherwise an unauthorized individual is able to enter the default value of PIN or Master PIN through accessing user's KeyA token and then he/she accesses user's secure partitions.

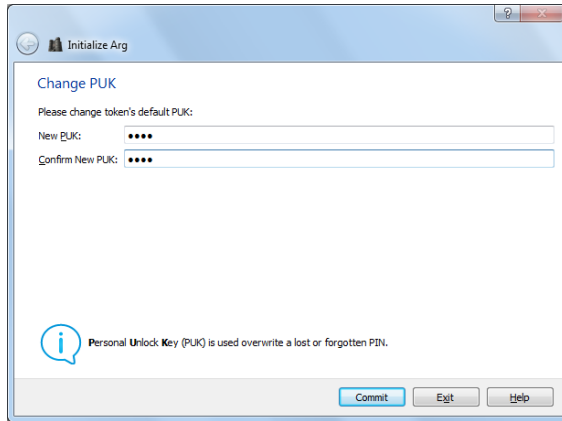


Figure 6- Change PUK (KeyA3 token)

6.3 Create New Profile

If your token is being used for the first time, it contains no profile and you should create a new profile (Figure 7).

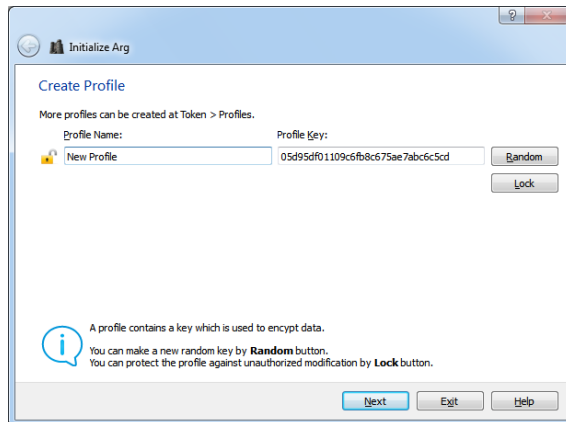


Figure 7- Create a new profile

Choose a name for profile in profile name part and enter its key in the profile key part.

Random key button causes a random key to be created for profile which can also be changed by user.



Lock button locks the profile that you have created. This part is explained more in section Profiles Management.

By pushing the next button the window of Figure 8 will be shown. User can save a new profile as an external file.

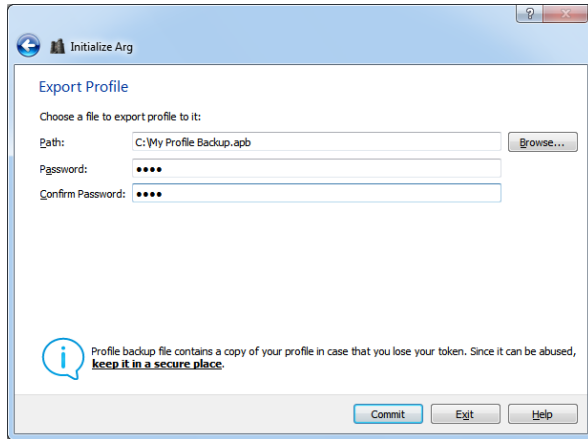


Figure 8- Create backup from new profile

Notice: there is always the possibility that program token be lost or damaged, therefore the secure partitions that have been created by the profiles existing in this token are probable to be irrecoverable. To solve this problem, user may get a new token and enter the profile backup file on it by the use of Arg software. Refer to section Profiles Management for more explanation.

6.4 Create a Secure Partition

In this step you are able to create a secure partition by following these steps (Figure 9).

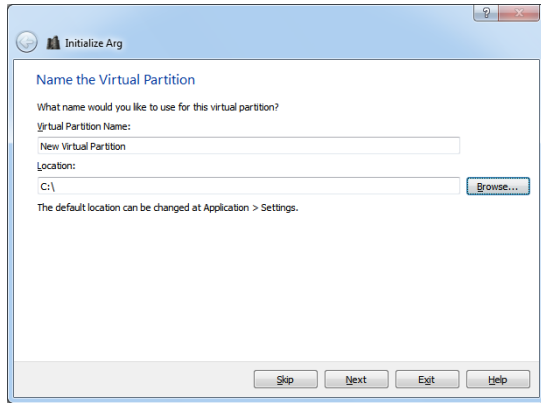


Figure 9- Specify new virtual partition name and path

After specifying partition name and location, you may go to the next step (Figure 10) and specify the partition size and file system type.

If you click the *Skip* button, the operation that creates new virtual partition will be stopped, but other settings such as changing PIN, Master PIN and profile creation will be stored.

You may change size and file system type of your partition according to your need. More explanation is mentioned in section Create Secure Virtual Partition.

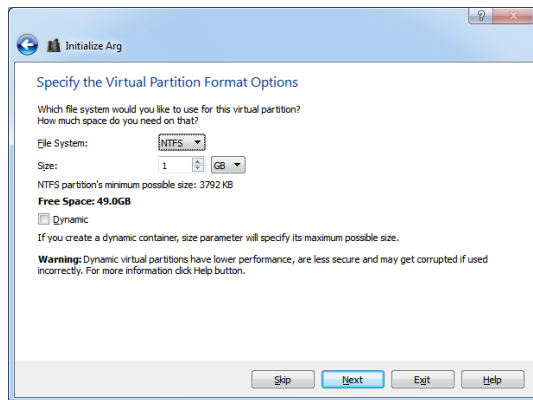


Figure 10- Specify new virtual partition format options



In the next step the profile by which your partition is intended to be encrypted will be specified (Figure 11).

In this step not only you may use the profile you have created in previous steps, but also you can change the profile which is used to encrypt secure partition by clicking on profiles management link.

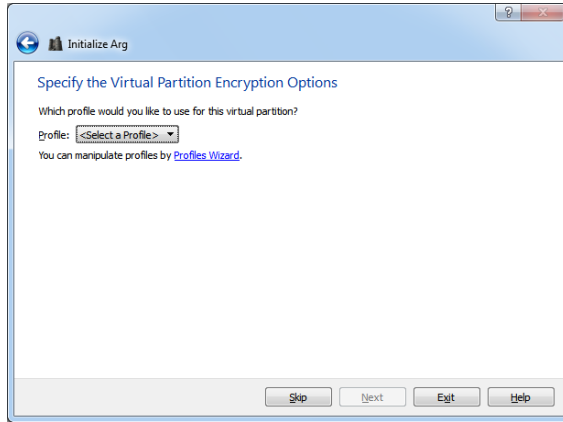


Figure 11-Choose new virtual partition's profile

After applying size, file system, physical location and other partition settings, you should select a file as a backup. This file contains information about the partition that enables you to recover valuable information when the partition is impaired (Figure 12).

Note: this file doesn't store any information about partition data.

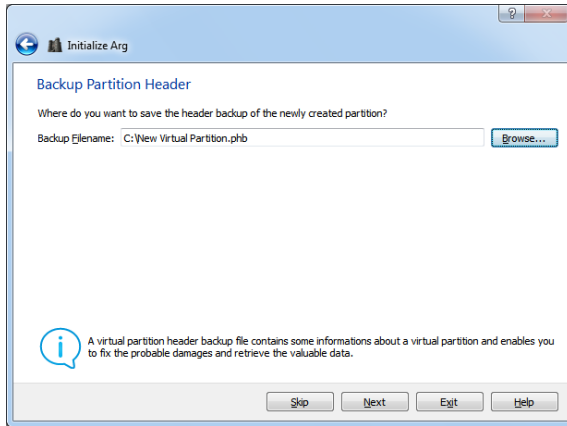


Figure 12- Create backup from partition header

In the next step (Figure 13) you can observe all the settings you have applied for virtual partition, and virtual partition will be created by clicking on Format button.

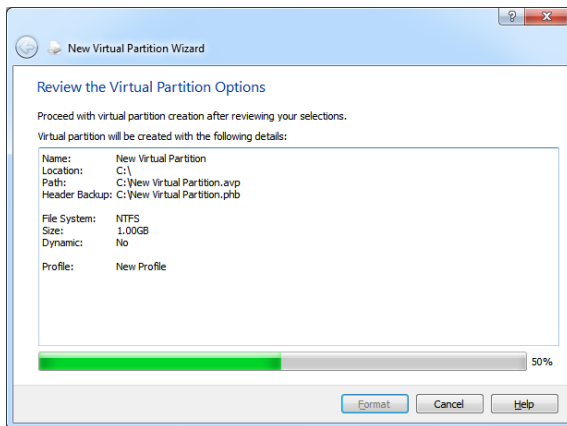


Figure 13- Show settings of creating new virtual partition



In the last step (Figure 14) you may see all changes which have been done up to now. If the system couldn't have registered a setting, the setting is specified by red sign.

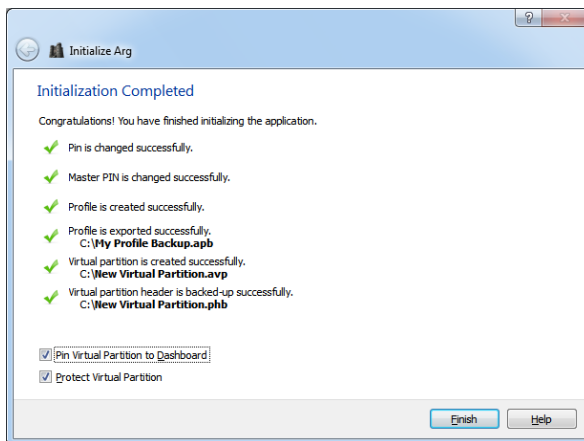



Figure 14- Display primary configuration results to user

7 Software Settings

Arg software settings consists of settings about secure partitions and mounting them which can be accessed through Application | Settings menu or  icon from program toolbar.

7.1 General Settings

In this part (Figure 15) there are several settings for automatically dismounting the partitions that have been mounted and warning messages. The settings are:

The option of *Forcibly dismount all partitions when screen saver is launched*: this causes the mounted partitions to be dismounted after displaying *screen saver* page.

The option of *Forcibly dismount partition if not being used for _ minutes*: this results in dismounting partition if a specific data is not written in (or read from) that.

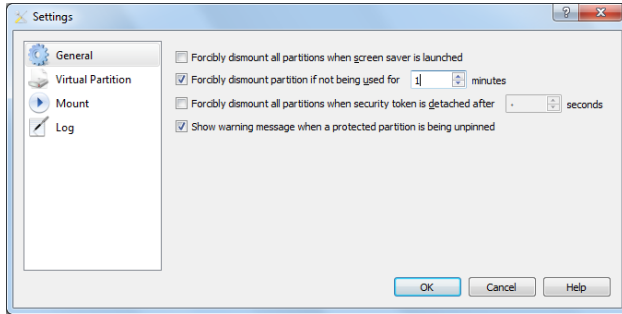


Figure 15- General settings window of software settings

The option of *Forcibly dismount all partitions when security token is detached after _ seconds*: it leads to dismount all partitions after, the duration of time that you specify, detaching token from computer. If you inactivate this option, all partitions will remain mounted after detaching token.

The option of *Show warning message when a protected partition is being unpinne'd*: it leads to show warning message if a protected partition is being unpinne'd. By unpinne'd a protected partition, it is not protected anymore and may be deleted.

7.2 Virtual partition Settings

User is able to specify a default path for *Arg* software where the virtual partition image file is to be saved while being created (Figure 16).

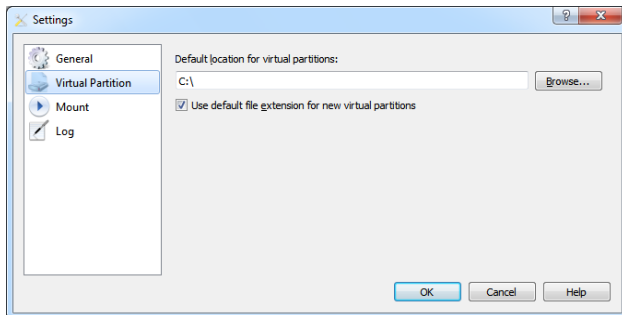


Figure 16- Virtual partition window of software settings



If the option of *Use default file extension for new virtual partitions* is selected, *avp* suffix will be added to the new virtual partition's name when it is being created.

7.3 Mount Settings

While mounting a secure partition which has not been pinned to dashboard, multiple choices can be existed, such as the drive letter of secure partition after mounting (Figure 17). Moreover it can be specified that the partition data be in read-only mode; or that the drive resulted from mount be added to system drives list as removable. If *ask for mount options* is selected, these settings must be applied when a partition is being mounted. Refer to section Mount Secure Partition, for more information.

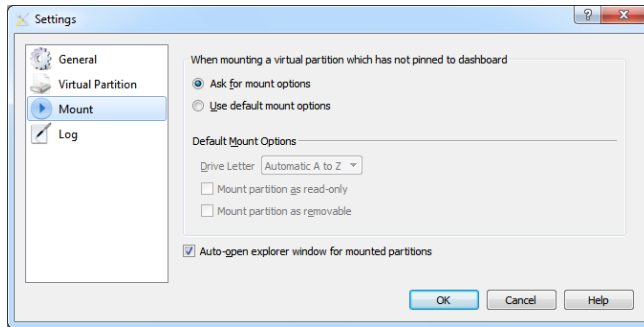


Figure 17- Mount options of software settings

Selecting the option of *auto-open explorer window for mounted partitions* causes the related partition *Explorer* window and its contents to be opened for you after mounting a partition.

7.4 Log Settings

Arg software enables you to record log from software performance. To apply log settings, select *Log* part from settings window (Figure 18). In this part, you must specify the location to store log file and the log level. *Arg* software is able to record internal logs in multiple levels. By choosing higher levels (more details) of reporting, the lower levels are also covered. The levels are as followed:

Disabled: no kind of software performance or user log is recorded in this mode.

Fatal: only fatal errors are recorded in this mode.

Critical: only critical errors are recorded in this mode.

Error: this mode is to record any kind of error.



Warning: besides software errors, warnings are recorded in this mode. The software default mode is this mode.

Notice: only points that are to be noticed by user are recorded in this mode.

Information: all errors and software transactions with token are recorded in this mode.

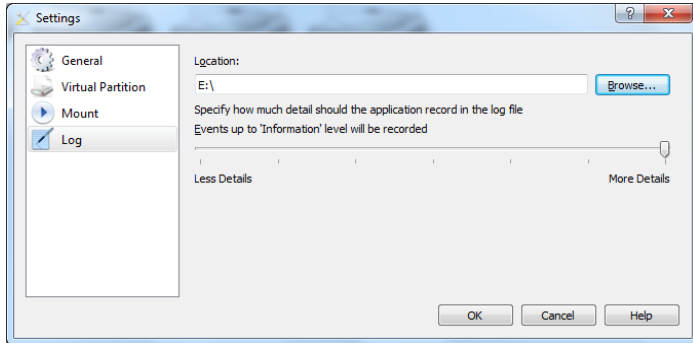



Figure 18- Log settings

8 PIN Management in KeyA Token

User can change KeyA token PIN. Moreover he/she can define new PIN for KeyA token or, change Master PIN or his/her *PUK*, by accessing Master PIN (in Key2 tokens) or *PUK* (in KeyA3 tokens). To do that, you should select *Change PIN* from *Token* menu or click on  icon from toolbar of the software main window (Figure 1). Therefore, the window of Figure 19 will appear for you.

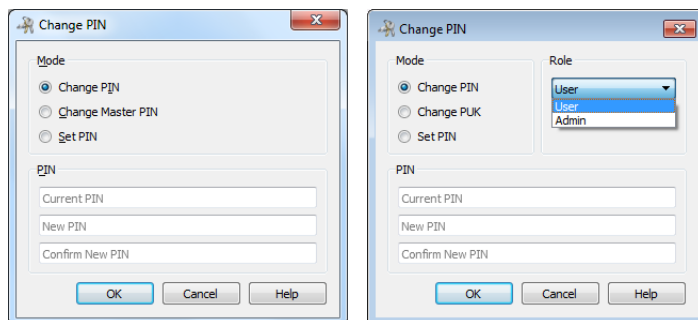


Figure 19- The window of changing PIN and PUK in KeyA3 token (right picture) or Master PIN in KeyA2 token (left picture)

8.1 Change KeyA Token PIN

To change user PIN in KeyA2 tokens, select change PIN option from the left picture and then enter the current PIN and the new one and confirmation of the new PIN.

To change PIN in KeyA3 tokens, first select change PIN option from the right picture and then choose the user role and enter current PIN and the new one and confirmation of the new one to record the settings for related user.

8.2 Change KeyA3 Token Admin PIN

To change Admin PIN in KeyA3 tokens, first select change PIN option from the right picture and then choose the admin role and enter current Admin PIN and the new one and confirmation of the new one to record the settings for related user.

8.3 Change KeyA2 Token Master PIN or KeyA3 Token PUK

To change KeyA2 Master PIN select change Master PIN option according to the left picture, and enter current, new and confirmation of new Master PIN.

To change PUK in KeyA3 tokens select Change PUK option according to right picture and then choose user or admin role. Then enter the current, new and confirmation of the new PUK to record the related user settings.

Warning: administrator must note that ten times of sequential entering wrong Master PIN or fifteen times of PUK causes the token to be locked. In this mode only the producer company (PayamPardaz) can redefine Master PIN or PUK.




8.4 Define Token PIN

In the cases that you have forgotten your KeyA2 module PIN, you may redefine a new PIN by Master PIN. To do that select set PIN option from the left window of Figure 19 and then enter current Master PIN, new and confirmation of new PIN.

If you use KeyA3 module and have forgotten your PIN or PUK, you may redefine them by having their related *PUK*. To do that, select set PIN option from the right window, then choose user role for setting new PIN or admin for setting new Admin and enter current related PUK, new and confirmation of new *PIN or Admin PIN* in order to record the related user settings.

9 Profiles Management

Arg software enables you to create or edit your profiles and then create backup from them and finally transfer profiles from backup file to token. To achieve that, select *Profiles* from *Token* menu or click on  icon from software main window toolbar to open profile window (Figure 20).

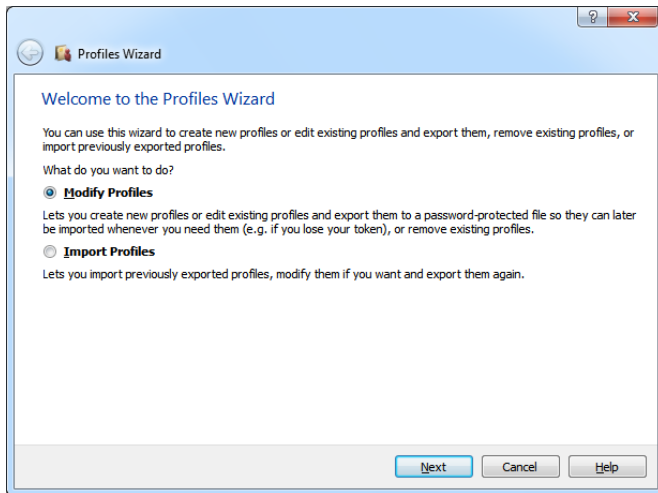


Figure 20- Profiles management window

9.1 Modify Profiles

If you want to create a new profile or edit current profiles, choose *Modify profiles* option from Figure 20 to display the window of Figure 21. In this page you may create, edit, delete or lock a profile. While locking a profile, it is



impossible for user to delete or change it. It is noticeable that in order to lock or unlock a profile, you need Master PIN (in KeyA2 tokens) or *Admin PIN* (in KeyA3 tokens). To create a random value for profile key, click on *Random* button. Also, user can make sure about the value randomness by changing at least one desired character.

Notice: it is obvious that user can modify profile keys that has not been locked by the administrator.

Notice: administrator must limit access to profiles before giving tokens to user to be used. Moreover, he/she must change default Master PIN or Admin PIN related PUK to make sure that user cannot access to them.

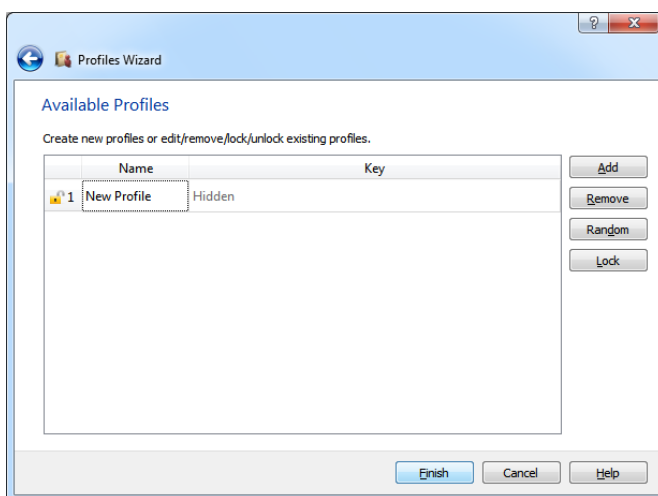


Figure 21- Profiles wizard window to modify profiles

Since it is impossible to recover a secure Partition's data when it's profile is being deleted (e.g. due to changing the key of a profile saved in token or being lost or impairing KeyA token), therefore you should keep a copy of the created or changed profile in a secure location after creating a new profile or changing existing profiles. Accordingly, in the window of Figure 21 after creating or editing the related profile, the *Finish* button will be changed to the *Next* button and you will be directed to the window of Figure 22 by clicking on it.

In this window you must choose a name and password to encrypt the file. It is recommended that you choose a password which is easy to be remembered since profile backup file is rarely used.



Warning: if you want to change partition profile, first you should transfer the data inside the partition to a overt drive and again transfer the copied data after creating another secure partition with the new profile to it. If you change a profile without passing the mentioned steps, the previous secure partitions cannot be used.

Notice: it is impossible to read profile from token.

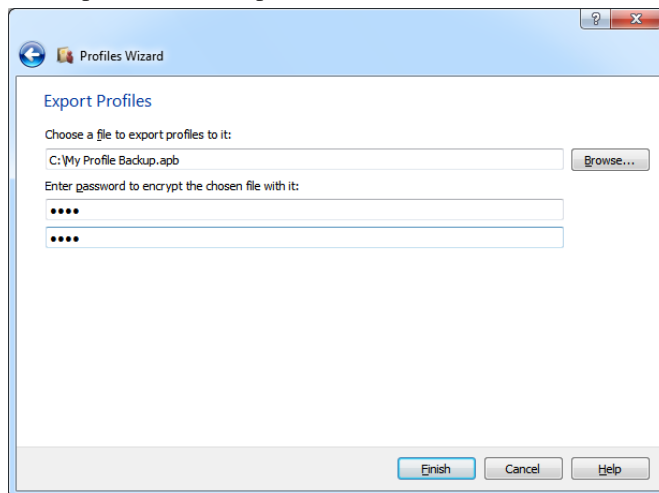


Figure 22- The window of creating backup from new profile

Notice: if you intend to share the created secure partition(s), you must securely share the profile with your contacts.

9.2 Import Profiles from Backup File to Token

If you want to reuse the profiles that you have created and now you are storing them in an external file, choose *Import Profiles* option from Figure 20 and click on next button to observe Figure 23. Select the file containing profile and enter its password. If the file contains a valid profile, the profile list becomes updated and the window of Figure 21 will be displayed again.

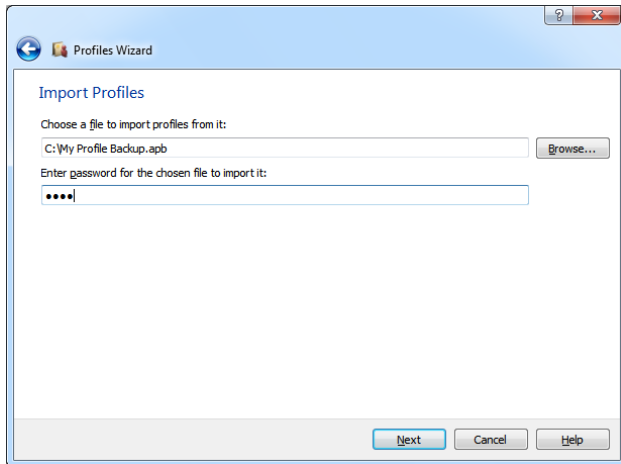


Figure 23- Import profiles window

9.3 Upgrade From Hoda Software to Arg Software

If you previously used Hoda software, and now you want to upgrade your software to Arg, it is necessary to introduce the encryption keys existing on your old token to Arg Software. To do that, select *Upgrade Profiles* from *Token* menu (Figure 3) before software login, the window of Figure 24 will be displayed.

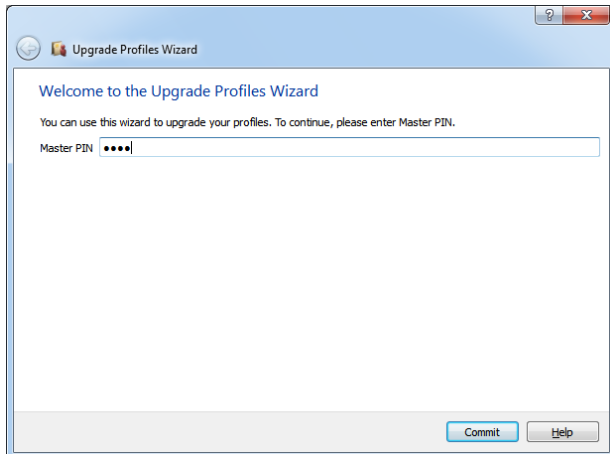


Figure 24- Upgrade profiles window



In this window you must enter Master PIN (in KeyA2 tokens). By clicking on send button you will be directed to the next page and all keys existing on your token will be displayed to you (Figure 25). Notice that if you mention explanation while creating Hoda encryption keys, these explanations will be shown in the name part of each profile.

Notice: encryption keys in Hoda software are started from 0 index but they are shown from 1 index in Arg software. As a result the encryption key number 1 in Hoda software shows index 2 in the window of Figure 25.

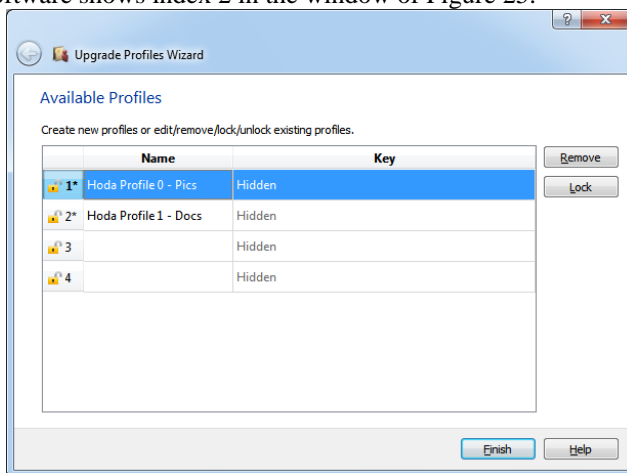



Figure 25- The encryption keys on token with their explanations

If you are sure that there are some invalid encryption keys among them you may delete them by clicking *Remove* button. By clicking on *Finish* button, the new changes will be applied and the existing encryption keys will be upgraded to Arg profiles.

Warning: user must pay attention that which of the existing encryption keys he/she has used in Hoda software. If the user unconsciously deletes a key by which a partition has been encrypted and finishes the operation, the information cannot be recovered.

10 Create Secure Virtual Partition

A secure partition is a secure drive that is virtually created on computer by Arg software and the information inside the partition are stored in an image file.

To create a secure partition on computer, select *New Virtual Partition* from *Partition* menu or choose  icon from the toolbar of the program main



window (Figure 1) or right click on an empty space of dashboard and select *New Virtual Partition*.

Then a window will be opened that enables you to create a new partition in several steps. The steps are as follows:

First according to Figure 9, define your image file name and path, locally or on network. *Arg* software saves virtual partition image file with *avp* suffix by default. If you want to save the files without any suffixes, you must change their virtual partition settings in 7.2 part. If none of the fields is empty you may go to next page (if you want to choose a Persian name for your virtual private partition, there are some explanations which are mentioned in section *Change a Partition's*).

In the next page (Figure 10) specify file system type as *FAT32* or *NTFS*. Note that if you select *FAT32*, there would be limitations, such as the maximum size of the file which can be created on partition is *4GB*, or the partition minimum volume is *292KB* and the maximum capacity is *16TB*.

If you use *NTFS* system file, the minimum partition volume is *3792KB*.

If dynamic option is selected, the created partition is dynamic from volume point of view. The difference of this mode with standard mode is that image file volume in dynamic mode is equal to its real content and the free space isn't filled with random values. This means that in spite of standard mode, the whole space considered for the partition is not taken from file system, while creating the partition. By information volume increase in partition, the allocated space for its volume will be increased accordingly. Of course the maximum partition volume is the value considered for it while it is being created.

After choosing secure partition size and its file system type settings, you should select the profile by which the partition must be encrypted (Figure 11). Not only you are able to use existing profiles, but also you may create new profile by clicking on profiles management link and use the created profile.

In the next page (Figure 12), you must select a file as secure partition header backup. This file contains information about the partition which enables you to recover its valuable information while the partition header is being impaired (refer to part *Create backup from header*, for more information). After selecting backup file for new partition, all of your selections will be displayed (Figure 13). If *Format* button is clicked, an image file with the size of secure partition will be created in the specified path.

In the last page (Figure 26) a message that shows the end of secure partition creation will be displayed to user. There are two options in this page, you can add this partition to the list of protected partitions by choosing *Protect Virtual Partition*. Protected partitions are those which cannot be deleted, renamed and



changed randomly. If the user wants to change, rename or delete them, he/she must extract them from protected files list by Arg software.

By choosing *Pin Virtual Partition to Dashboard*, the secure partition that

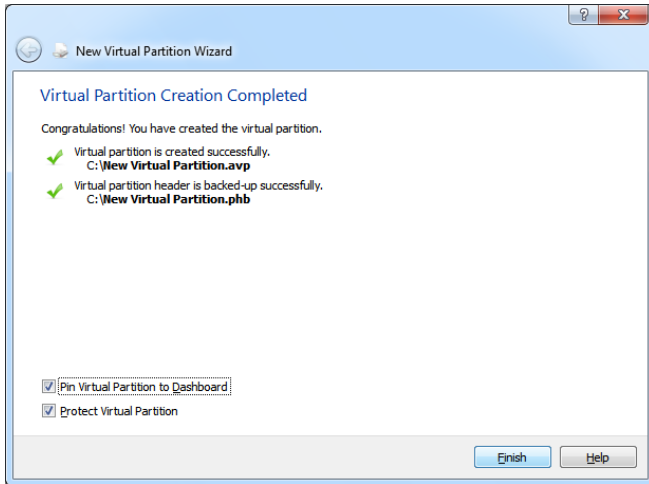



Figure 26- New virtual partition creation completion message

you have just created will be located on software main page. Notice: if you want to create a secure partition on a read-only media like CD or DVD, first create it on hard disk and then copy it on the qualified media.

11 Pin Virtual Partition on Dashboard

To mount virtual partition or use other Arg software facilities and tools, a partition must be chosen. To do that, the partition must be pinned on software dashboard. To achieve that follow one of the bellow methods:

Click on  icon of program toolbar in the main page. As a result, a window will be opened for you to choose partition(s).

Right click on an empty space on dashboard and run the command of *Pin Virtual Partitions* on dashboard. As a result, a window will be opened for you to choose partition(s).

Run the command of *Pin Virtual Partition*, from *Partition* menu. Then again, a window will be opened for you to choose partition(s).


After running each of the above steps your selected partitions will be pinned on dashboard.



12 Mount Secure Partition

To use and access secure partition information, it must be mounted first. To do that follow one of the bellow methods:


1. If a partition is Pinned on dashboard it can be mounted through one of the following processes:

Select the partitions from software dashboard and run *Mount* command from *Partition* menu. Click on  icon from the program toolbar in main window (Figure 1).

Double click on one of the dashboard partitions.

Right click on partition(s) and run *Mount* command.

2. If there are no partitions on dashboard, you may mount a virtual partition through the following steps:

Select *Mount* from *Partition* menu or click on  icon from program toolbar.

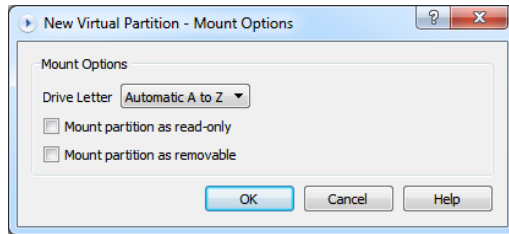


Figure 27- Partition mount options

Select your virtual partition(s) from the appeared window. These partitions can be selected from network such as a *LAN* or Internet.

If you have not selected the option of “*use default mount options*” in *Mount* part of software settings, a window will be opened (Figure 27) for you to enter partition mount settings. Select your chosen drive letter. If you select the *Automatic A to Z*, software will select the first free drive letter of system. If you select the *Automatic Z to A*, software will select the last free drive letter of system.

If you choose the option of “*Mount partition as read-only*” in the above window, the related partition will be mounted as read-only.



If you choose the option of “*Mount partition as removable*”, the partition will be mounted as removable such as a flash memory and *Recycle Bin* and *System Volume Information* branches will not be created in it.

If the partition has been already mounted without selecting the option related to removable partition and has been mounted as a standard tool (not removable), it is probable that the mentioned branches be created in the partition due to user’s operations such as deleting a file of partition. In this mode the partition will be mounted as a standard tool even by selecting the mentioned option.

13 Partitions Automatic Mount

It is possible to mount one or several partitions automatically while login process is being done in *Arg* software. To do that, you must choose the partition as your favorite partition. To select a partition as your favorite partition follow these steps:

First pin the partition to dashboard (refer to section Pin Virtual Partition on Dashboard for more explanation).

Click on the star sign of the partition right side, then it goes yellow (Figure 28).



Figure 28- Select partition as favorite partition


From now, the favorite partitions will be mounted when *Arg* software login process is being done.



14 Change a Partition's Properties

First pin the partition on dashboard (go to section Pin Virtual Partition on Dashboard for more explanation). To access partition's properties follow one of the methods:

Right click on the partition and click on *Properties*, then the window of Figure 29 will be displayed.

Select the partition and click on  icon.

Select the partition. Then select *Properties* from *Partition* menu.

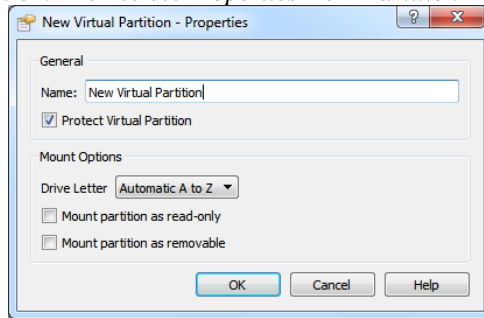


Figure 29- Partition properties window

You may rename partition in this window or change the protected mode of partition image file to unprotected mode (more explanations are mentioned in section Protect Secure Virtual Partition Image File). Other mount options are explained in section Mount Secure Partition.

When you entered a new name for partition, it will be renamed after clicking OK button but other properties changes will be registered after partition mounting.

Point: if you want to choose a Persian name for your virtual partition, the operating system language for non-English characters must be Persian. Otherwise, after renaming the partition, unrelated characters will be recorded as the partition's name. Nevertheless, the secure virtual partition is still usable. To activate this facility in Windows 7, follow the bellow path:

Click *Region and Language* from *Control Panel* to see Figure 30.

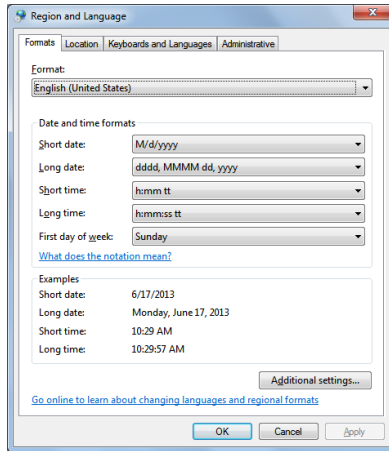


Figure 30- Region and Language window

Click on *Administrative* branch to see Figure 31.

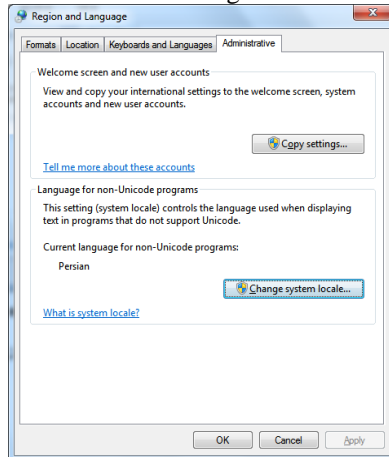


Figure 31- Administrative branch to change language

If the current language is not *Persian* in *Language for non-Unicode programs* part, click on *Change system locale* button and choose *Persian* language from the opened list.

15 Protect Secure Virtual Partition Image File

It is probable that secure virtual partition image file be deleted by the user or others intentionally or unintentionally. To solve this problem, image files can




be protected by *Arg* software. Therefore, it is impossible to access these files such as delete, rename and so on out of *Arg* program. To do that, right click on partition after pinning the partition on dashboard, and select Properties to see the window of Figure 29. By checking *Protect Virtual* Partition option, you can protect secure partition or inactivate it from protected mode.

Point: note that the secure virtual partition is protected until it is pinned on dashboard, and it can be deleted or renamed after unpinning it from dashboard.

16 Dismount Partitions


To inactivate a partition and remove it from system active drives list, follow one of these ways:

Select your partition and click on  icon from software main page toolbar.

Right click on your partition and select *Dismount* option from the opened menu.

Select the partition and choose Dismount option from *Partition* menu..

To dismount all secure partitions follow one of the bellow processes:

Click on  icon of software main page toolbar.


Right click on program dashboard and select *Dismount All* option.

Select *Dismount All* from *Partition* menu.

17 Unpin Partitions from Dashboard

After finishing the operations on secure partitions, user may prefer to unpin them from dashboard and substitute them with new partitions. To do that follow one of the bellow methods:

Select the partition from dashboard and right click on it. Then select the *Unpin Virtual Partition*.

Select the partition from dashboard and click on  icon of the main page toolbar.

Select the partition from dashboard and then choose *Unpin Virtual Partition* in *Partition* menu.

18 Share secure virtual Partitions

It is possible to share a partition in *Arg* software in order to be used by several people. To do that, first its image file must be shared with the individuals in the network. It is necessary for all individuals who want to use this partition to have the profile that encrypts the mentioned partition and



mount it in a read-only way. For more explanation about the way of mounting a partition in read-only way, refer to section Mount Secure Partition.

Point: all users must mount the shared partition in read-only way. If a user mounts it with write and read facilities, others cannot mount it and they face an error message while mounting.

19 Tools

In *Arg* software, there are various tools to use facilities and capabilities of the software. The tools and their performances are explained as follows.

19.1 Create backup from header

Usually each file is threatened by the danger of change, due to hardware problems such as suddenly power shut down or software problems such as computer viruses. Since the most important part of a secure partition is its header, which is located at its beginning and it is impossible to recover the stored information without its correct value; therefore an extra header is created automatically at the end of partition. Moreover, for more confidence, *Arg* software has tools to create a backup file from header as an external file. So, if a header partition gets damaged, we can access the partition's information by restoring header backup.

First choose the partition, from whose header you want to create backup, from dashboard and click on *Backup Header* from *Partition* menu to see the window of Figure 32. Then in backup file part, select the file address in which you want to store backup file. If this file has not existed before, it will be created in continue.

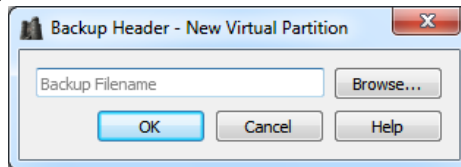


Figure 32- Backup header window

19.2 Restore header

This tool is used when it is impossible to read the partition contents due to the unintentional changes of the partition header. If the partition header which is located at the beginning of the partition is impaired, the partition can be recovered by the use of backup file which has already created by partition backup header creator tool.



Select the partition with impaired, then, click on *Restore Header* from *Partition* menu. Then you have the window of Figure 33. Select the address of header backup file related to the partition and click on OK button.

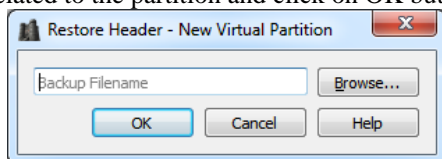



Figure 33- Restore header window

20 Exit

To prevent accessing *Arg* software facilities or immediately dismounting all secure partitions, you must logout software. To do that, follow one of the following methods:

Eject KeyA token from *USB* port.

Click on  icon in the toolbar of the main page.

Select *Logout* from *Application* menu.

To completely exit software, right click on program icon in *Tray Icons* and choose *Exit*. You can also click on *Exit* from *Application* menu.

Notice: the program will not exit by clicking *Close* button of the software main page, only the main page will go out of access. Therefore, you may reopen it by clicking on the program shortcut on desktop or by running *Show* command in *Tray Icons*.