**Traffic** Safety and **Security Division**

3M Center, Building 235-3A-09

St. Paul, MN 55133-3225 [www.3M.oom/mvss](http://www.3M.oom/mvss)

3M™ AVERAGE SPEED CAMERA SYSTEM KEY MANAGER USER MANUAL ISSUE 2.0

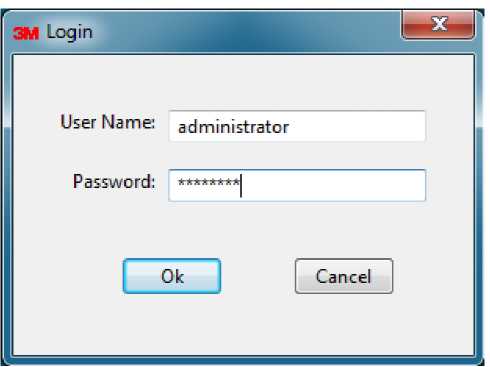
AMENDMENT RECORD

|  |  |  |
| --- | --- | --- |
| ISSUE | DATE | BRIEF DETAILS OF CHANGE |
| 1.0 | 17/07/2009 | Initial Release |
| 2.0 | 09/07/2013 | Update to 3M nomenclature for products |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

The overall issue status of this document is the latest issue shown in the table above. Authors: Qifeng Huang

**1. User Account**

A user must login with user name and password while the 3M™ Average Speed Camera System Key Manager (KM, formerly also known as SpeedSpike Key Manager) starts as shown in figure 1.



**Figure 1 KM login**

Three levels of user account may be set up in KM following the windows paradigm.

* User
* Browse, query and generate cameras and shared secrets
* Browse and generate keystores
* Issue/reissue shared secrets and keystores, and track issue history
* Edit its own user account
* Administrator
* Add/Remove/Edit Users
* Imports camera details from Enforcement Manager
* Backup system data
* System Administrator
* Add/Remove/Edit administrators and users
* See passphrase history for all issued CD’s
* Generate ‘Recovery CD’ for Session Manager
* Recover system from a backup CD

The password of System Administrator and the SM/ERCU serial must be set up when KM starts for the first time, as shown in figure 2. By clicking "User Accounts” button on

"System Key Store” page, the users account management GUI will be presented as in figure 3.

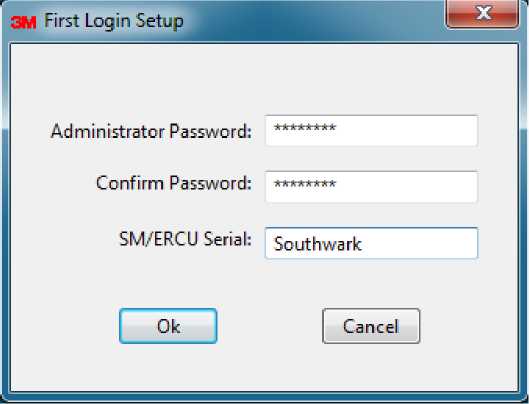


Figure2 KM first run setup

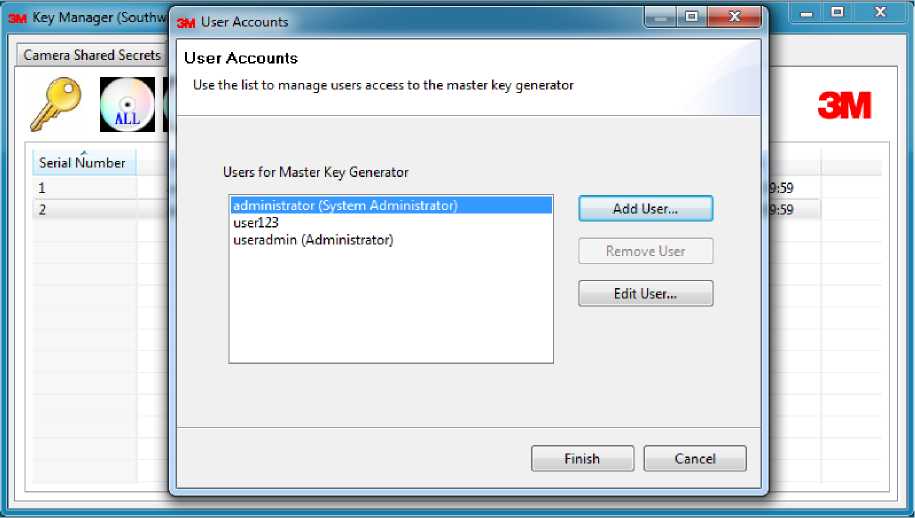


Figure 3: User accounts management

Add/remove/edit operations are accessible for the user with the granted privileges. As an example, the add user operation screen is shown in Figure 4. A unique username, a password and optionally whether it will be an administrator, if the operator logins as a system administrator, should be provided to add a new user account.

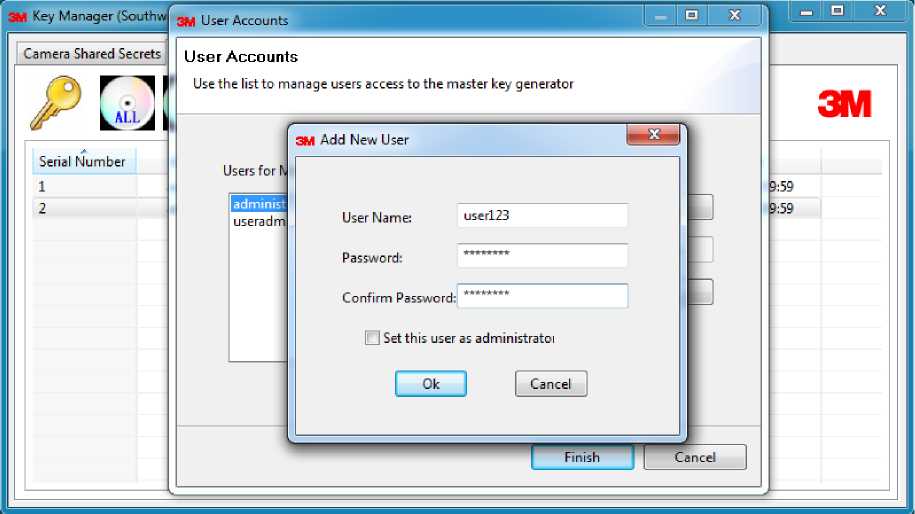
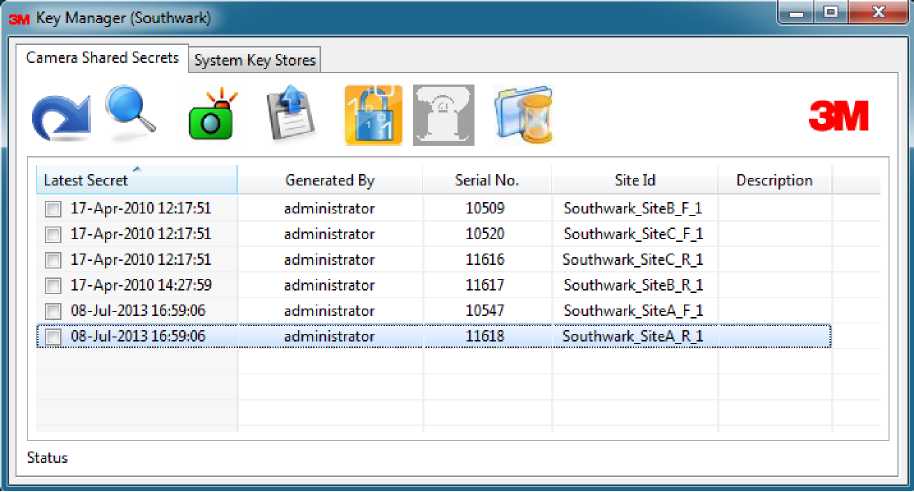


Figure 4 Add a new user account

Please note: to apply use account changes, the operator needs to click the "Finish” button in the use account management page to exit.

2. Camera Shared Secret



Camera shared secrets is part of the fundamental instation-outstation security. Consistent shared secret should be encrypted and retained on both the camera and SM sides.

The Camera Shared Secret summary status is shown in figure 5 with fast action buttons for common user operations, which include:

* "Populate All Cameras”: it will populate all cameras retained in the system and show their details in the display panel.
* "Query Cameras”: As shown in figure 6, query retained camera details based on serialNo’s or serialNo range, separated with space or comma. The results can be either displayed in a new panel or with new cameras appended to the current list.

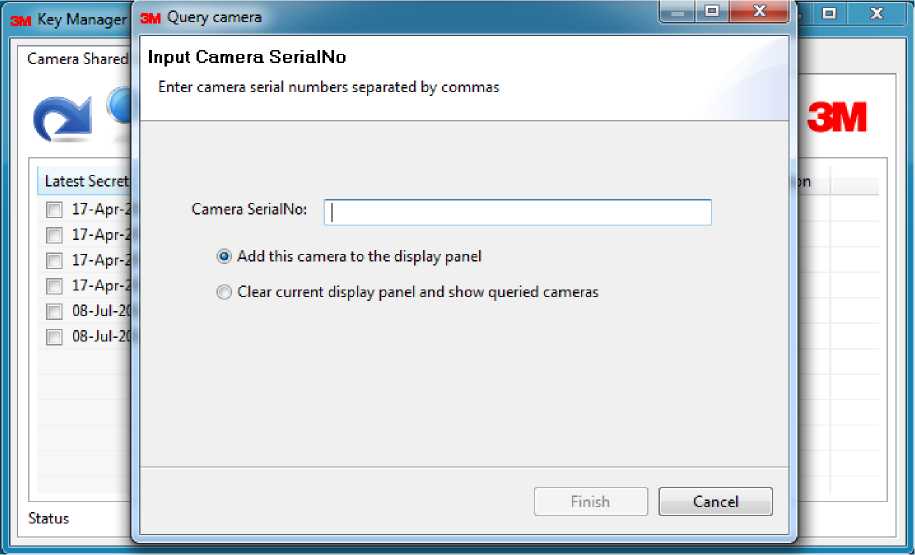


Figure 6 Query camera details

> "New Camera”: As shown in figure 7, KM allows users manually to add cameras into the system, and optionally generate and/or issue shared secret if they so wish. If "issue secret CDs” option is set, an additional page will pop out during the process to set up pass phrases protecting the issuing CD’s. just follow the on­screen instructions to finish the process.

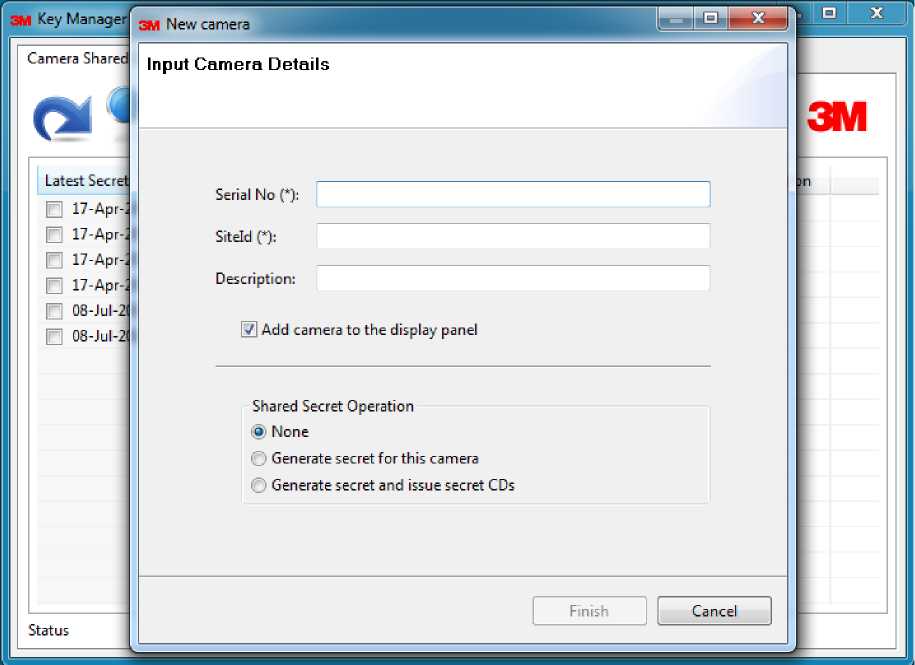
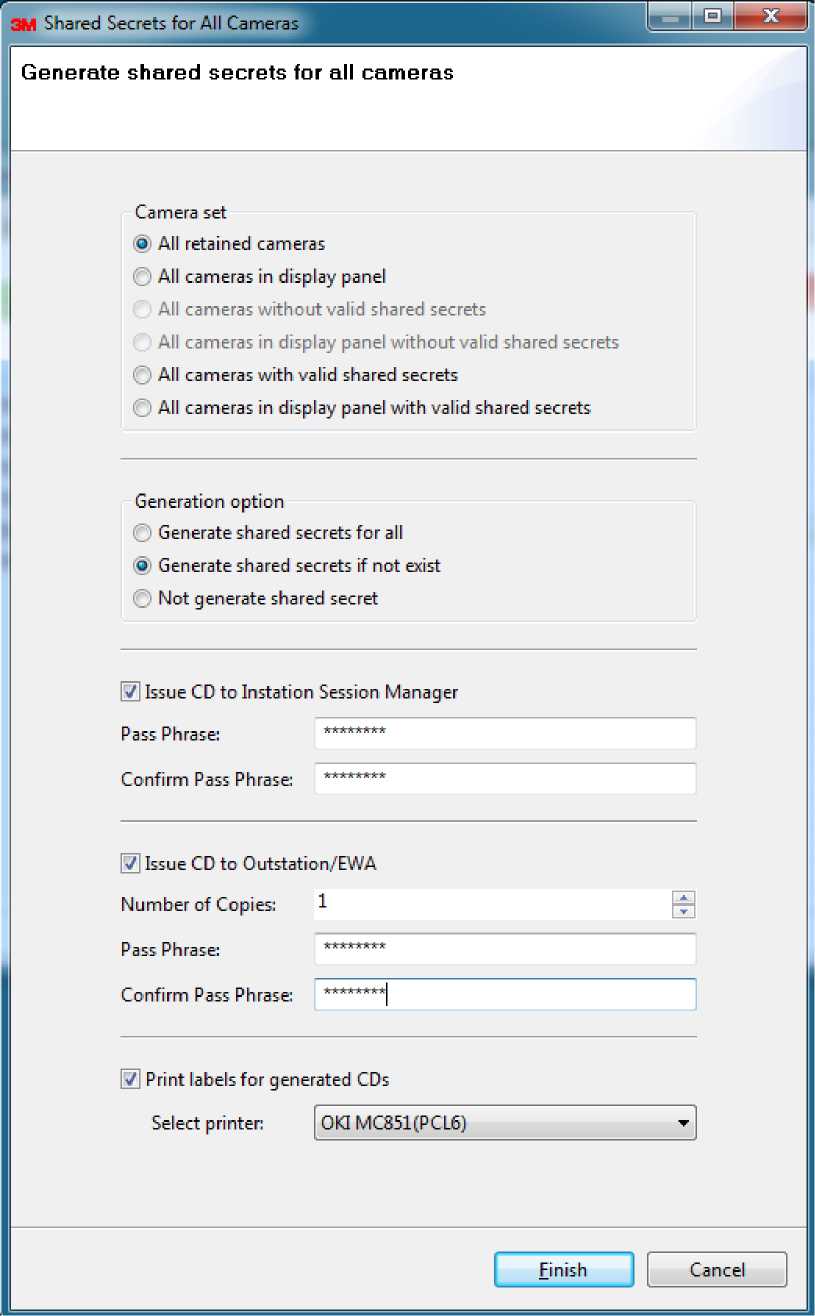


Figure 7 Add a new camera

* "Import Cameras”: this operation is only available to administrator or system administrator, which imports cameras details coming from Enforcement Manager into the system.
* "Secrets for All”: A comprehensive operation for either all retained cameras or all cameras shown in the main display panel. As shown in figure 8, the camera set included in the operation is set in the first radio group, and under what condition a new shared secret will be generated for a particular camera is set in the second group. The operator could also choose whether the latest shared secret for each camera in the selected camera set should be issued to the SM and/or the outstation, their protecting pass phrases, CD copies, and whether CD labels will be printed from a selected printer.



* "Secrets for Selected”: similar to "secret for all” operation, but only applies to selected cameras in the main display panel.
* "Issued Secret Sets”: By clicking this button, you will go into the page to manage all historic generated/issued shared secret sets, as shown in figure 9. For each set, new CD’s including exactly the same set of shared secrets can be issued to SM/outstation again. A warning message will be popped up if any included camera has a newer generated shared secret since this set has been generated. The operator can also check full CD issue history information, and the system administrator can optionally check the pass phrase for each CD if its login password confirmed, as shown in figure 10. The "Get camera details” button operation will populate all camera details into the main display panel, highlighting cameras with updated shared secrets.

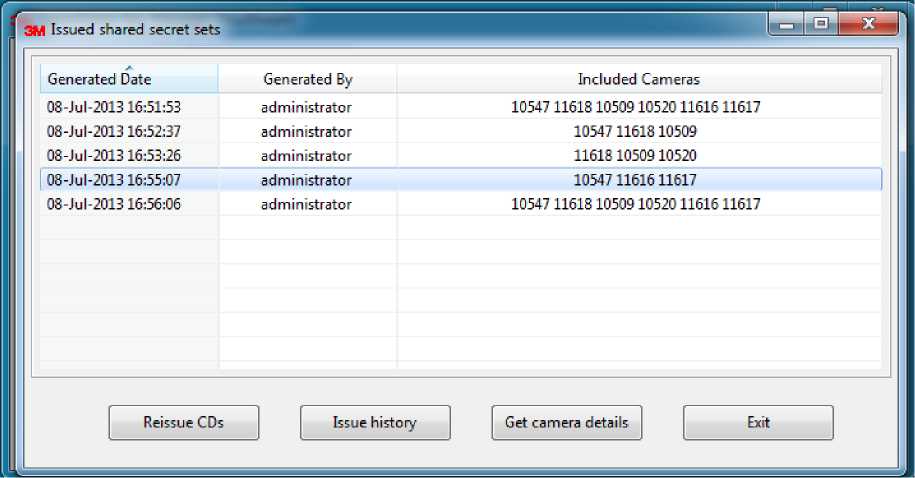


Figure 9 Issued shared secret sets management

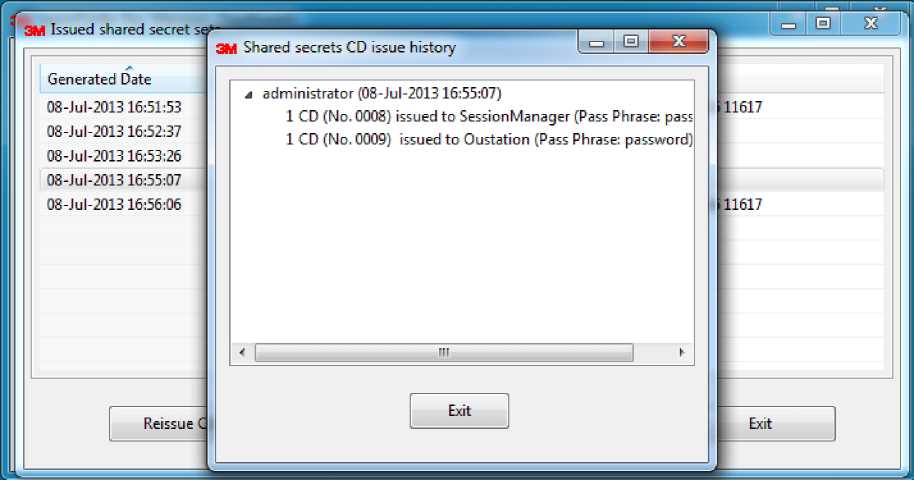


Figure 10 Track shared secret set issue history

From right mouse popup menu, it is also possible to show the whole secret generation history for a particular camera as shown in figure 11, or even to delete a camera if a shared secret has never been generated for this camera.

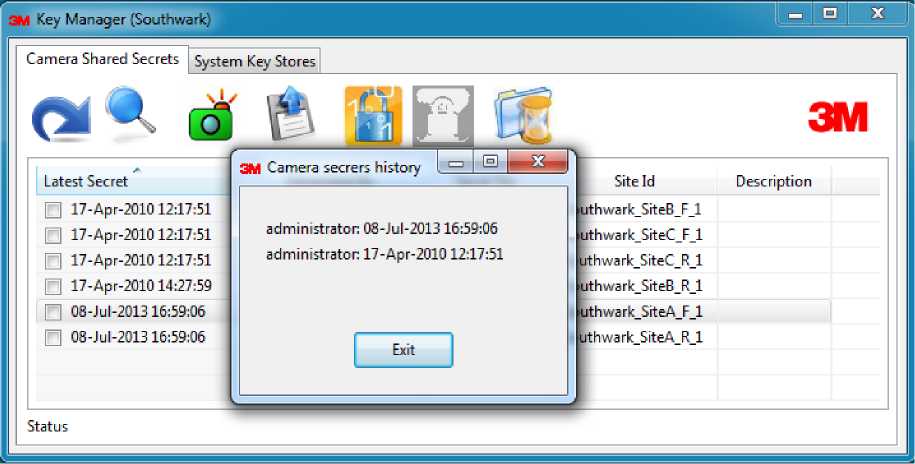


Figure 11 Camera shared secret generation history

3. Key Store Management

3M™ Average Speed Camera System uses RSA-2048 based public-private key pair as the fundamental machine-to-machine security, and also use AES-256 based symmetric

keys as the fundamental mechanism to protect very critical information such as camera shared secrets and session keys. The basic function of the key store management includes: to generate all key pairs and symmetric keys; to wrap related keys together and distribute them to SM, ERCU, OVDS and EM, each with a single key store protected with pass phrase. The Key Store Management summary screen is depicted in figure 12.

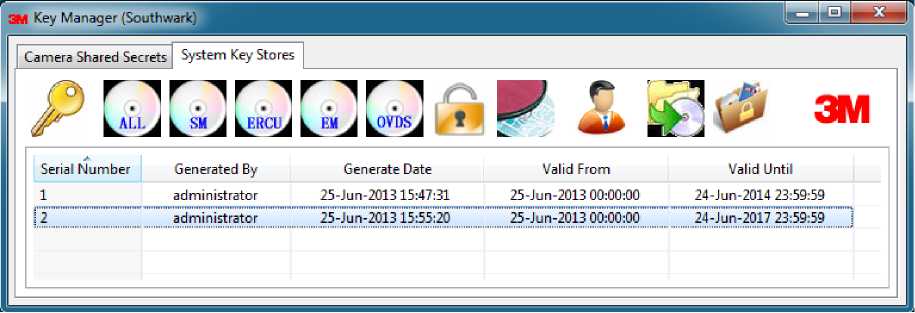
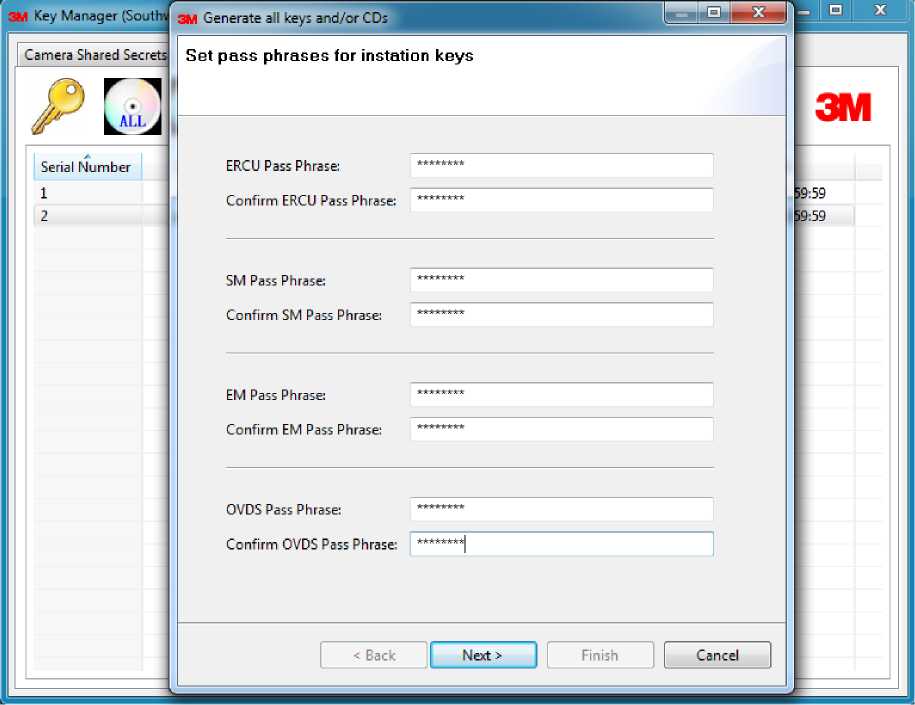


Figure 12 Key store management summary screen



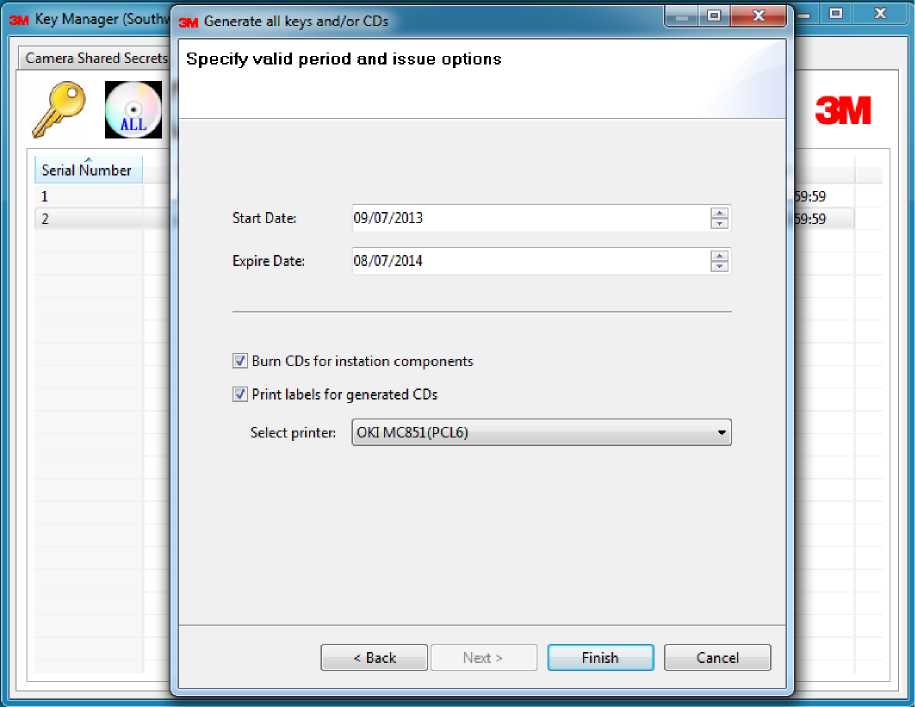


Figure 14 Set key store validity period and issue option

The process of generating a key set is shown in figure 13 and figure 14. You should set up the pass phrase for each individual key store. Corresponding pass phrase is required whenever a server/PC side component (Sm, ERCU, OVDS and EM) starts. A common valid period for all generated key stores should also be set as shown in figure 14. The instation can’t come into enforcement before this validity period and must be refreshed for continued operation after it. Optionally, you can burn these key stores into CD’s and print CD labels following the instructions popped out, which will then come across the air-gap and delivered to the instation machine to be loaded or updated.

You can also burn all four or one particular CD’s for a generated key set later. This process is shown in figure 15, which will issue the key store with serial number 3 to SM. Similarly, you can also check full CD issue history for each key set, and the system administrator can optionally check the pass phrase for each CD if its login password confirmed, as shown in figure 16 and figure 17.

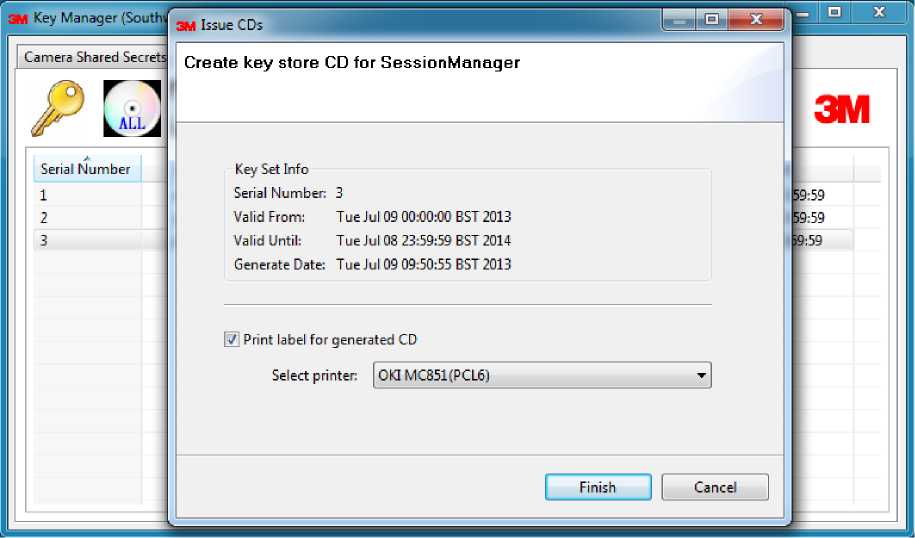


Figure 15 Issue key store CD to SM

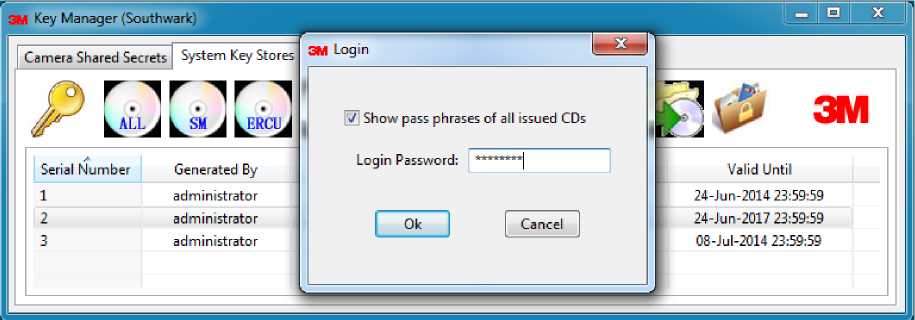


Figure 16 Confirm the administrator password

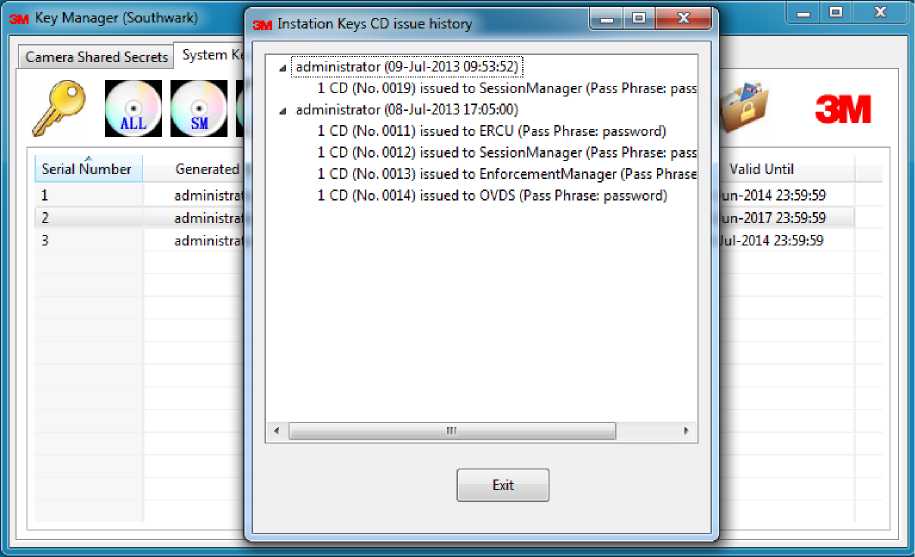


Figure 17 Key set store issue history

It is recommended that the instation key stores should be changed at least once a year, and are used in historic sequence. Changing key store in SM involves some critical operations to update retained shared secrets and session keys, which need to use access keys in old key store to decrypt data and use access keys in new key store to re-encrypt them. KM provides a function to issue a special "Recovery CD” to SM. This CD contains all necessary historic access keys, and the SMDL will automatically update the system to the current keystore using this CD irrespective of which keystore is currently loaded or something goes wrong for the key store SM currently used.

Given key stores and shared secrets managed by the KM play an important role in the the 3M™ Average Speed Camera System, KM provides additional functions to do data backup and recovery, which can only be performed by administrator or even system administrator (for data recovery), as shown in figure 18 and 19, respectively. We recommend you do a backup operation right after a new key set is generated and at a regular basis. However, data recovery should only be done for some serious reason and under 3M professional support, as you might lose some or even all the changes made to the system since the backup has been done.

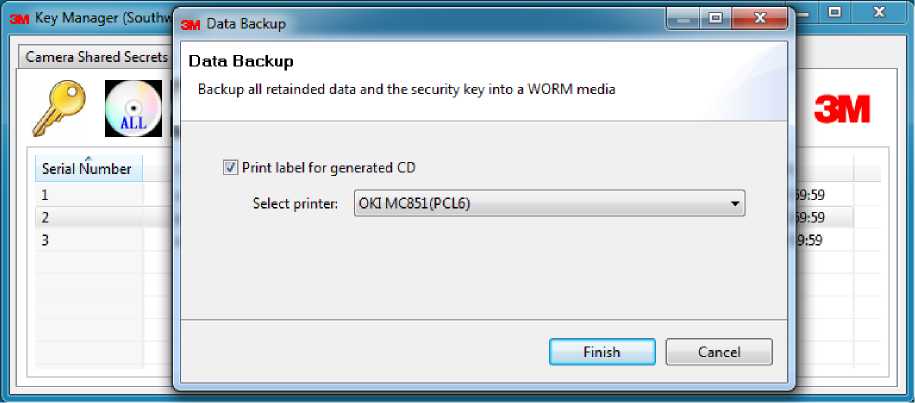


Figure 18 Data backup

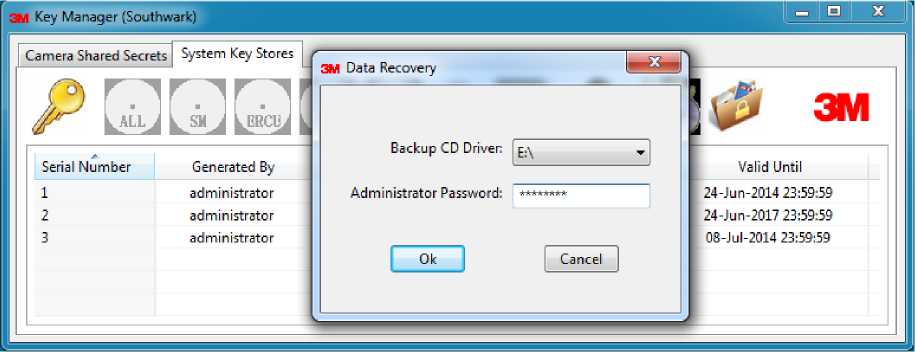


Figure 19 Data recovery

Appendix: Configurations in KM

Some configuration can be set in file $KeyManager/conf/ key-manager.properties, which are shown as follows (you can ignore the first part if you are using stated default settings):

#Configurations should be the same with these in EWA (in file ewa.ini):

ewa.secret.file = site\_100.enc ewa.camera.serialNo.column = 1 ewa.primary.secret.column = 2 ewa.trial.secret.column = 3

#Indicate the name of the CD-writer driver cd.writer.device = d: