**Отдел за безопасност на движението**

3M, сграда 235-3A-09

Ст. Пол, Минесота 55133-3225 [www.3M.oom/mvss](http://www.3M.oom/mvss)

3M™ СИСТЕМА ЗА УПРАВЛЕНИЕ НА КЛЮЧОВЕ НА КАМЕРА СЪС СРЕДНА СКОРОСТ

РЪКОВОДСТВО НА ПОТРЕБИТЕЛЯ

ИЗДАНИЕ 2.0

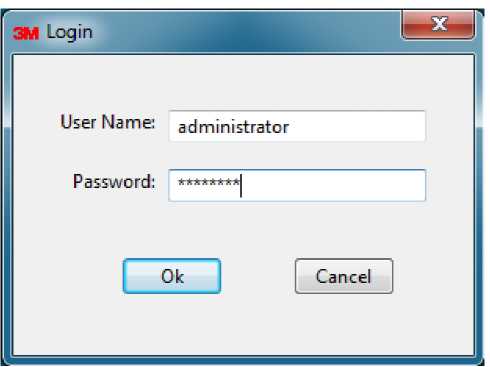
СПИСЪК С ИЗВЪРШЕНИТЕ ПОПРАВКИ

|  |  |  |
| --- | --- | --- |
| ИЗДАНИЕ | ДАТА | КРАТКИ ДАННИ ЗА ИЗВЪРШЕНАТА ПРОМЯНА |
| 1.0 | 17/07/2009 | Първоначална версия |
| 2.0 | 09/07/2013 | Актуализиране на 3М номенклатурата за продукти |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Настоящият документ представлява последното издание, показано в таблицата по-горе. Автори: Куифенг Хуанг

**1. Потребителски акаунт**

При стартиране на системата за управление на ключове на 3M™ камерата със средна скорост (КМ, позната преди като SpeedSpike система за управление на ключовете) потребителят трябва да се регистрира с потребителско име и парола, както е показано на фиг. 1.

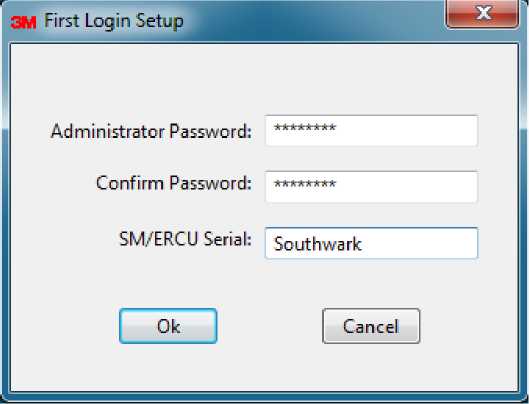


**Фиг. 1 Регистриране в КМ**

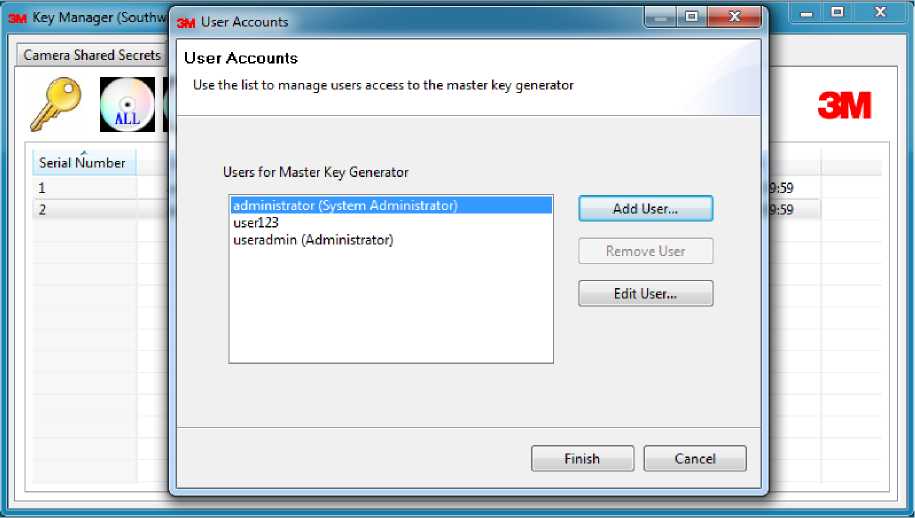
В КМ могат да бъдат зададени три нива на потребителски акаунти, като се следва парадигмата на Windows.

* Потребител
* Разглеждане, подаване на заявки и генериране на камери и споделени тайни
* Разглеждане и генериране на бази с ключове
* Издаване/повторно издаване на споделени тайни и бази с ключове, както и проследяване на историята на изданията
* Редактиране на собствения си акаунт
* Администратор
* Добавя/Премахва/Редактира потребители
* Импортира данни за камери от системата за управление на изпълнението
* Архивира системни данни
* Системен администратор
* Добавя/Премахва/Редактира администратори и потребители
* Вижда исторически паролите на всички издадени CD
* Генерира „възстановен CD“ за системата за управление на сесии (SM)
* Recover system from a backup CD Възстановява системата от архивирания CD

Паролата на системния администратор и серийния номер на SM/ERCU трябва да бъдат зададени при първоначално стартиране на КМ, както е показано на фиг. 2. При натискане на бутона “User Account” на страницата "System Key Store” се отваря потребителският интерфейс за управление на потребителските акаунти, както е показано на фиг, 3.

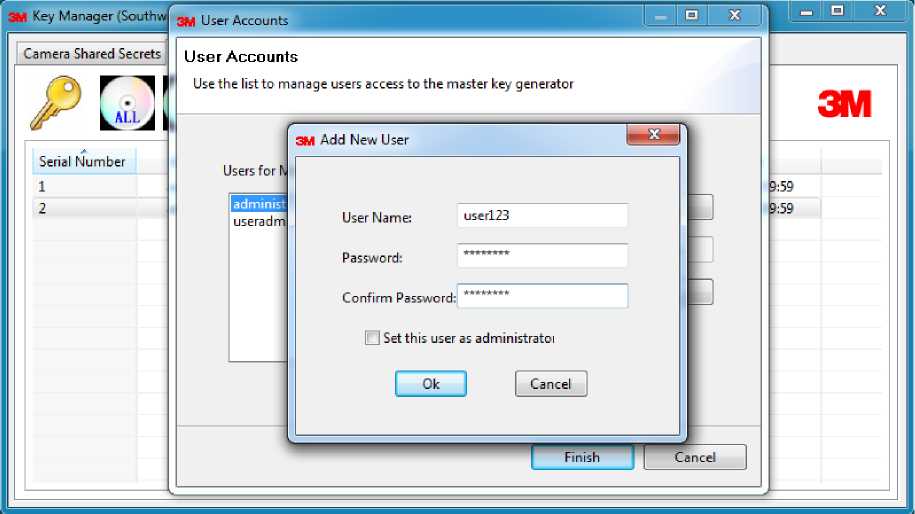


Фиг. 2 Настройване на първо пускане на КМ



Фиг. 3: Управление на потребителските акаунти

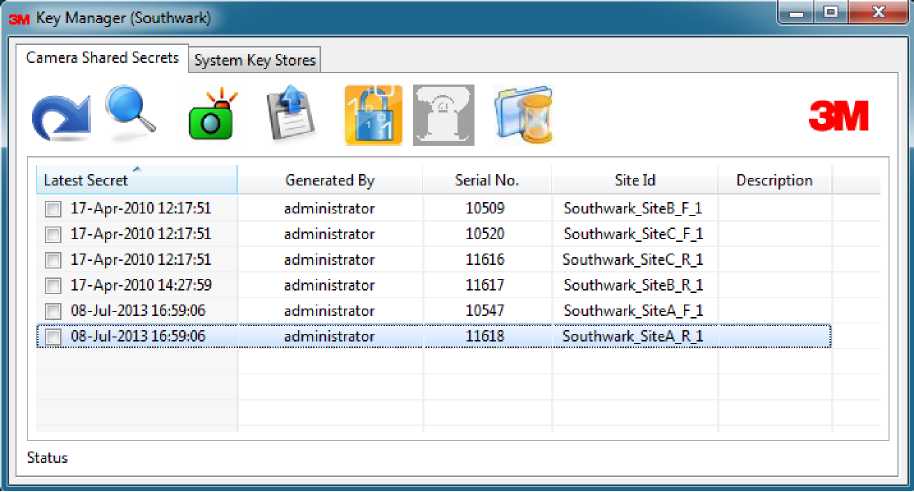
Операциите по добавяне/премахване/редактиране са достъпни са потребител със съответните привилегии. За пример е представена операцията за добавяне на потребител, показана на фиг. 4. За добавянето на нов потребителски акаунт е необходимо предоставянето на уникално потребителско име и парола, както и възможност за добавяне на този потребител като администратор, ако операторът се е регистрирал като системен администратор.



Фиг. 4 Добавяне на нов потребителски акаунт

Заб.: за да приложи извършените промени в потребителския акаунт, операторът трябва първо да натисне бутона "Finish” в страницата за управление на потребителски акаунти, за да излезе от нея.

2. Споделена тайна на камерата

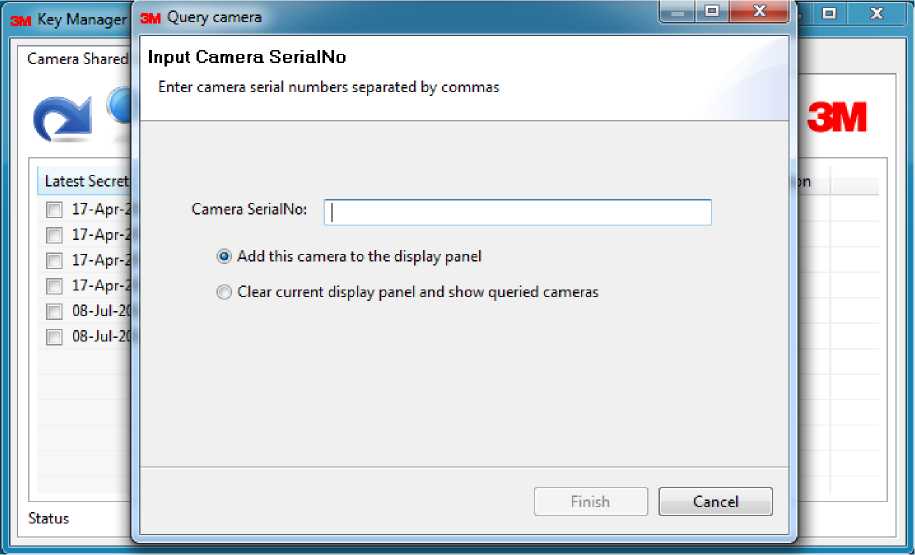


Фиг. 5 Основен прозорец на споделена тайна на камерата

Споделените тайни на камерата представляват част от фундаменталната вътрешно-външна сиг**у**рност. Съвместимата споделена тайна трябва да бъде криптирана и запазена, както на камерата, така и в SM.

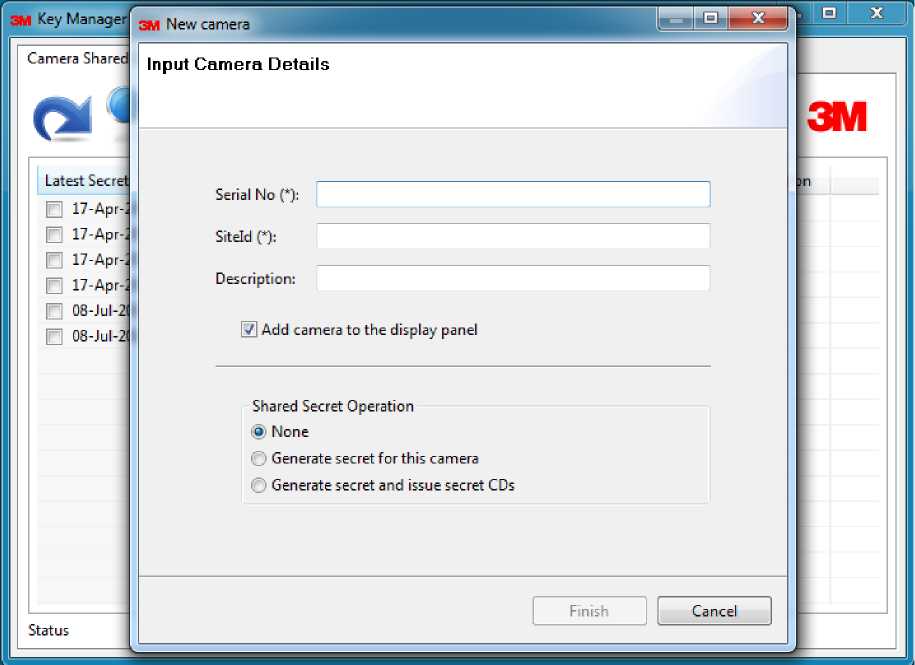
Обобщеното състояние на споделената тайна на камерата е показано на фиг. 5 с бързи бутони за обичайни потребителски операции, които включват:

* "Заеми всички камери”: заема всички камери, въведени в система, и показва техните данни в панел.
* "Заявка за камери”: Както е показано на фиг. 6, изпращане на заявка за данните на въведените камери на базата на серийните номер или серията от серийни номер, разделени с разстояние или запетая. Резултатите могат да бъдат показани в нов панел или с нови камери, добавени към настоящия списък.



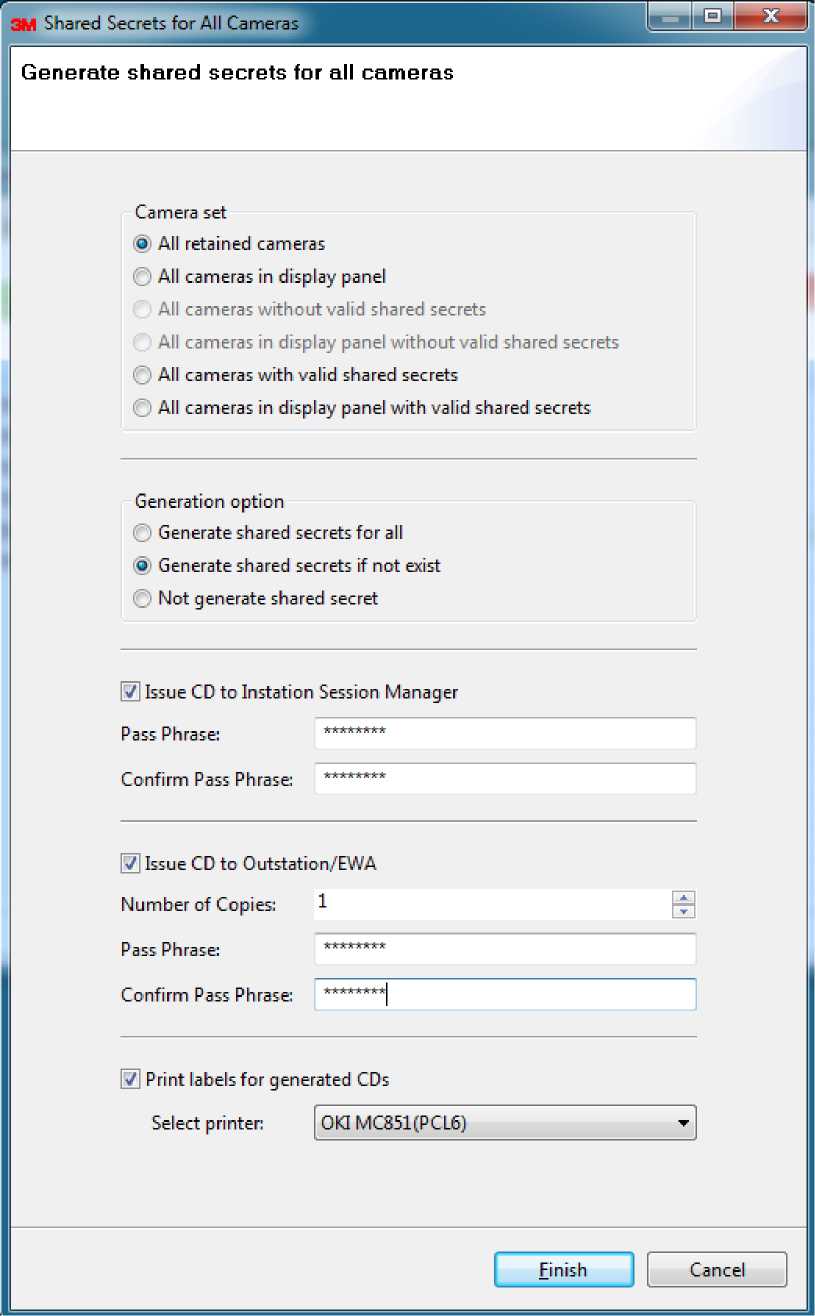
Фиг. 6 Заявка за данни на камера

> "Нова камера”: Както е показано на фиг. 7, КМ разрешава на потребителите ръчно да добавят камери в системата, както им дава и възможност да генерират и/или издават споделена тайна, ако желаят. Ако е зададената опцията "issue secret CDs” (издаване на CD с тайни), на екрана ще се появи допълнителна страница, на която да зададете паролата за защита на издадения CD. За да завършите процеса, просто трябва да следвате указанията на екрана.



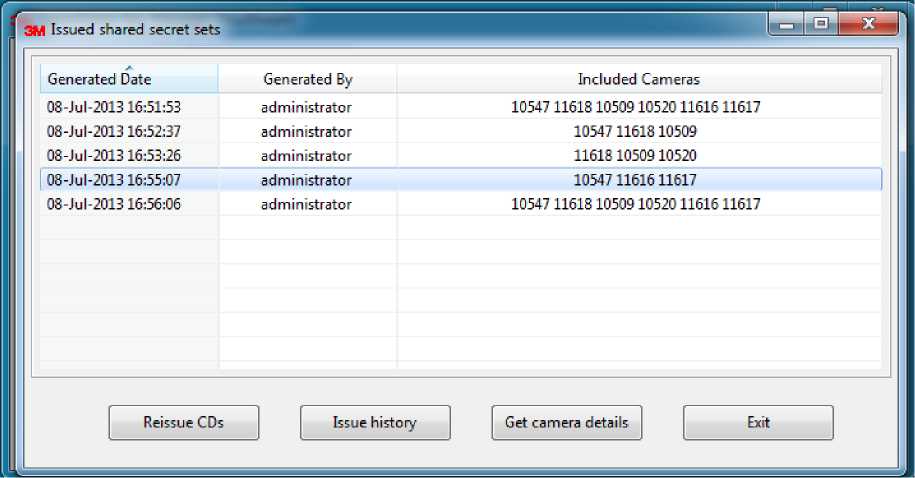
Фиг. 7 Добавяне на нова камера

* "Импортиране на камери”: тази операция е разрешена само за администратори или системни администратори, които импортират данни на камери, идващи от системата за управление на изпълнението (ЕМ) в системата.
* "Тайни за всички”: Цялостна операция за всички записани камери или всички камери, показани в основния панел. Както е показано на фиг. 8, групата камери, включени в операцията, е зададена в първата група с радио бутони, а във втората група радио бутони е включено при какви условия ще се генерира нова споделена тайна за конкретната камера. Операторът може да избере също дали последната споделена тайна за всяка камера в избраната група от камери трябва да бъде издаденa на SM и/или на външна станция, паролите за защита, CD копията, както и дали да бъдат отпечатани етикети за CD на избран принтер.

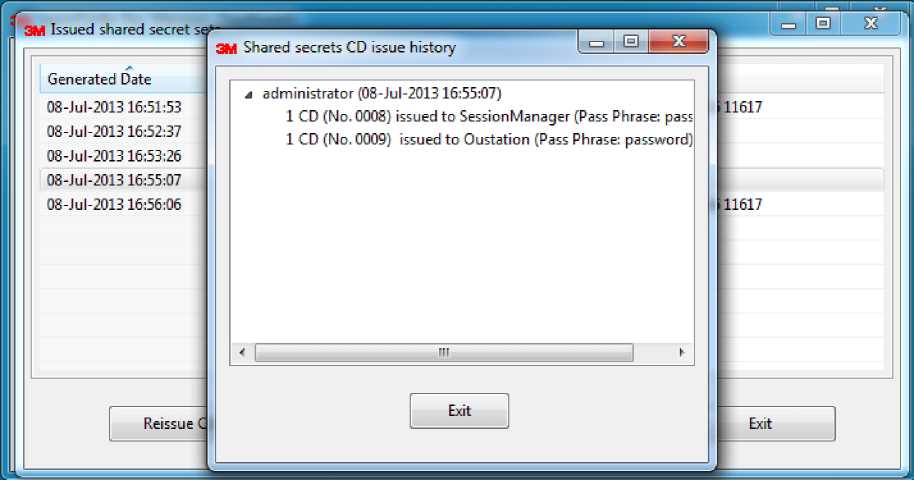


Фиг. 8 Генериране/издаване на споделени тайни за всички

* "Тайни за избрани”: подобно на предходната операция „тайни за всички“, но се отнася само за избраните в основния панел камери.
* "Издадени групи тайни”: При натискане на този бутон, влизате в страницата за управление на всички групи исторически генерирани/издадени споделени тайни, както е показано на фиг. 9. За всяка група може отново да бъде издаден нов CD, включващ точно същата група споделени тайни към SM/външна станция. На екрана се появява предупреждение, ако някоя от включените камери има нова генерирана споделена тайна спрямо момента на генериране на групата от тайни. Операторът може също да направи пълна проверка на историческата информация от издаването на CD, а системният администратор има възможност да провери паролата за всеки CD, ако паролата при регистрация е потвърдена, както е показано на фиг. 10. Операцията, която се стартира с бутона "Get camera details” (Получи данни за камерата) поставя всички данни на камерите в основния панел, като подчертава камерите с актуализирани споделени тайни.



Фиг. 9 Управление на издадените групи споделени тайни



Фиг. 10 Проследяване на историята на издаване на споделени тайни

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.

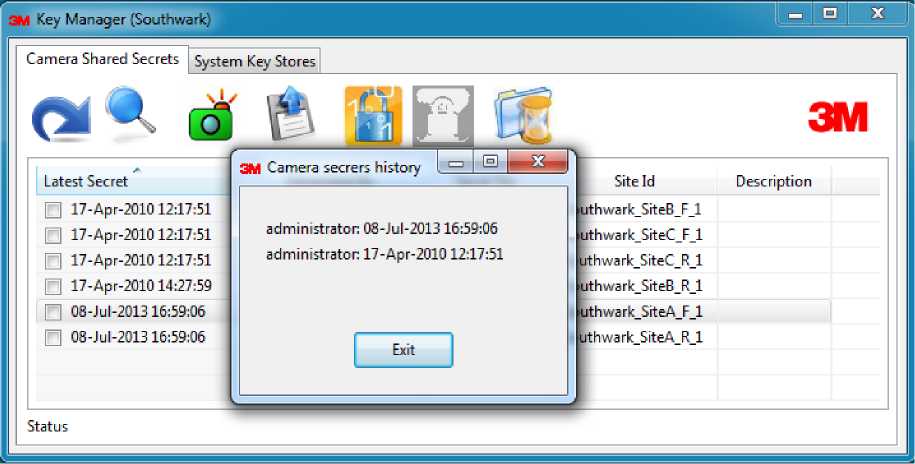


Figure 11 Camera shared secret generation history

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.

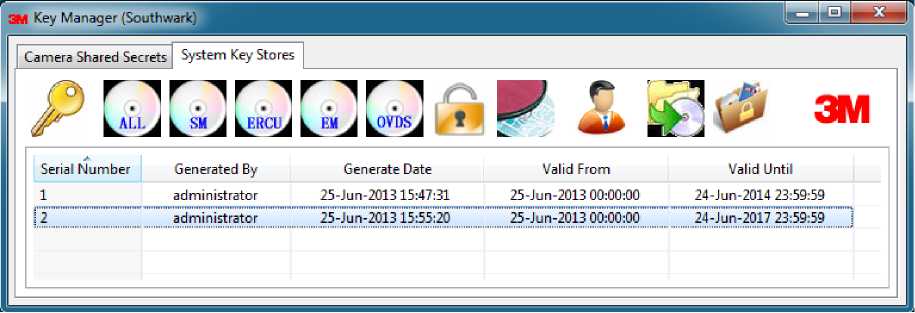
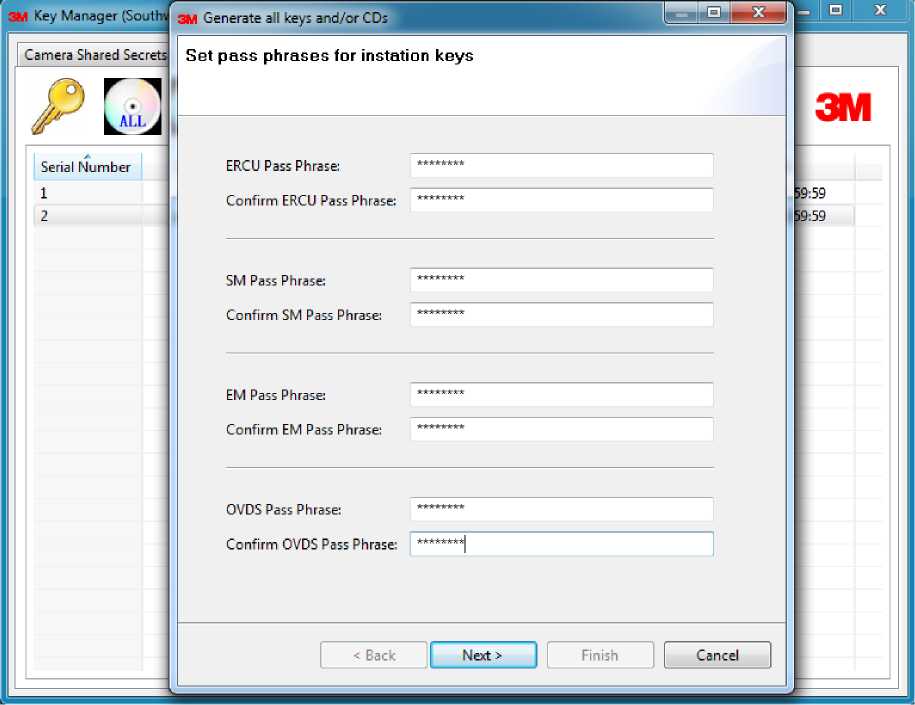


Figure 12 Key store management summary screen



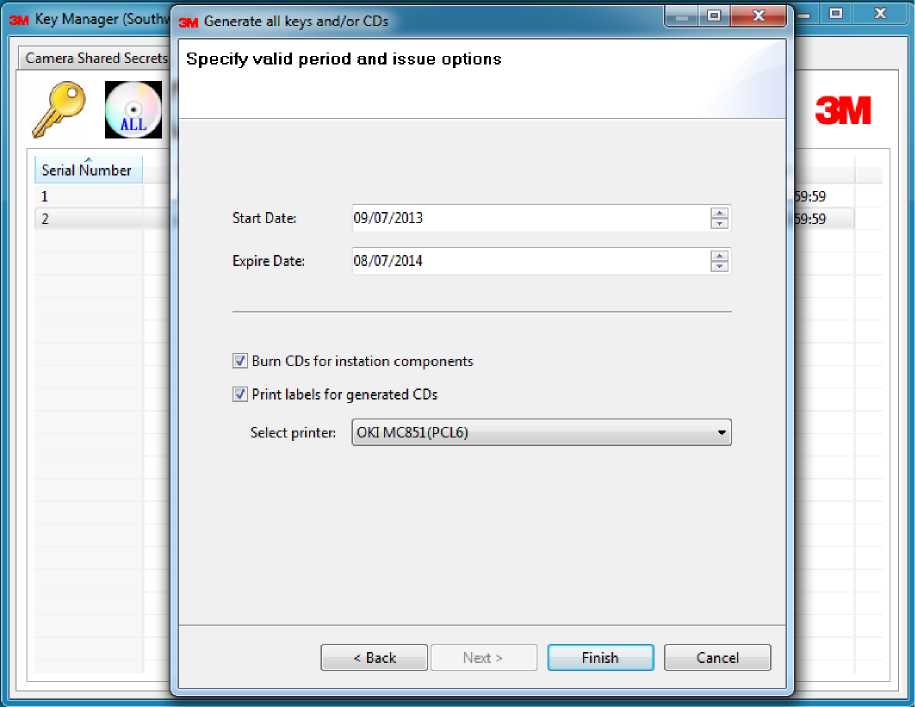


Figure 14 Set key store validity period and issue option

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.

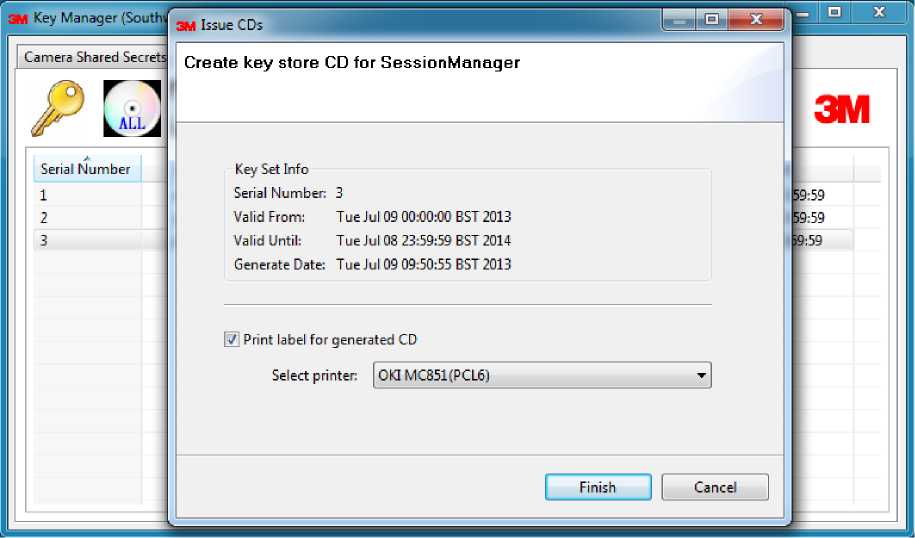


Figure 15 Issue key store CD to SM

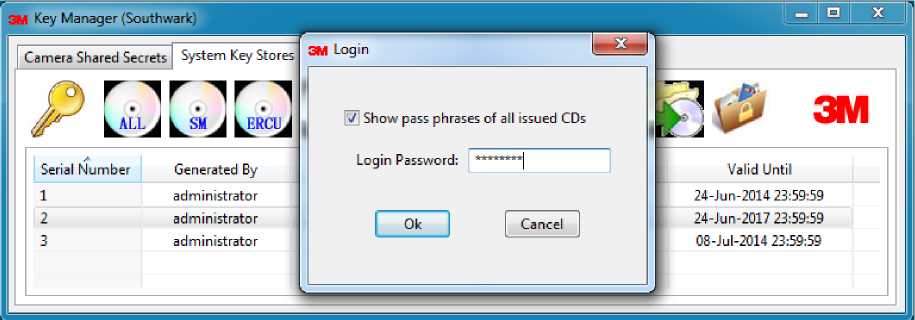


Figure 16 Confirm the administrator password

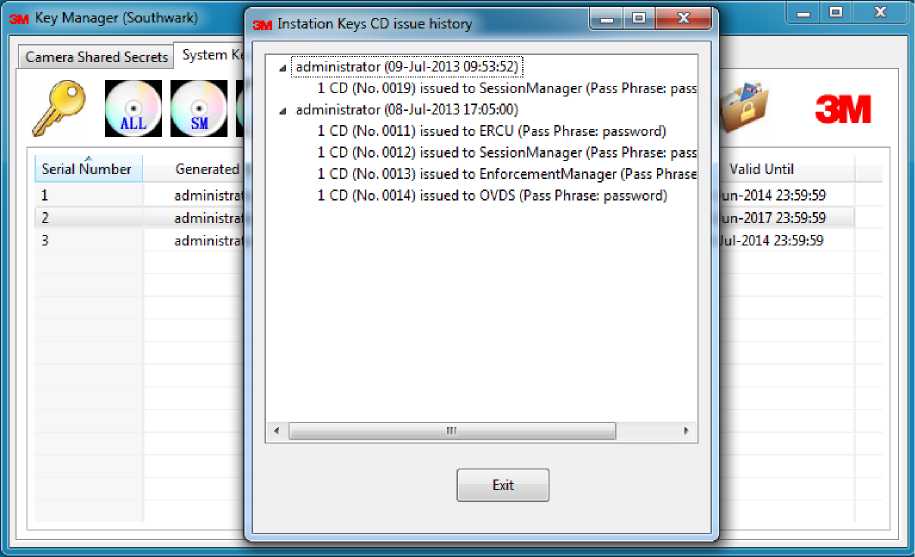


Figure 17 Key set store issue history

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.

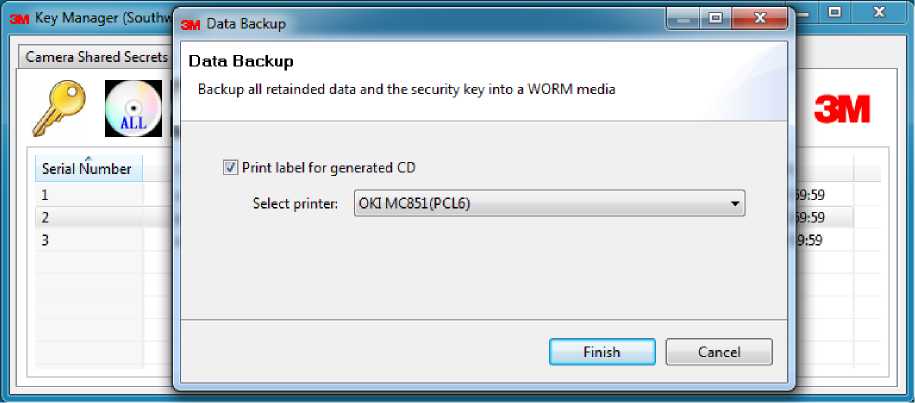


Figure 18 Data backup

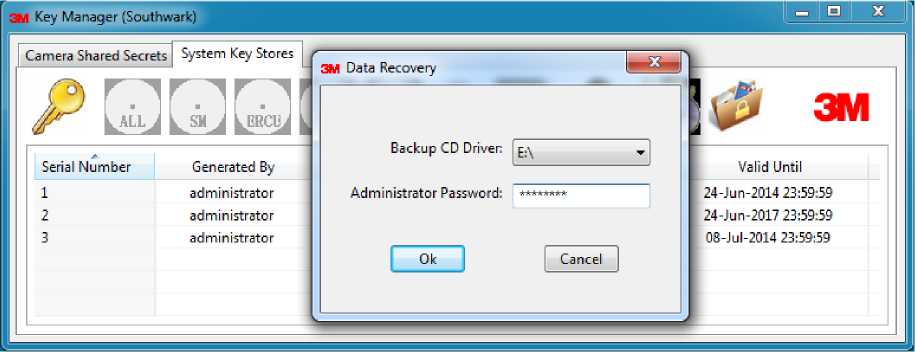


Figure 19 Data recovery

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: