

# UTILITIES MANUAL

*VERSION 1.0*



The Key to the Information Security

The data and information contained in this document cannot be altered without the express written permission of SecuTech Solution Inc. No part of this document can be reproduced or transmitted for any purpose whatsoever, either by electronic or mechanical means.

The general terms of trade of SecuTech Solution Inc. apply. Diverging agreements must be made in writing.

Copyright © SecuTech Solution Inc. All rights reserved.

WINDOWS is a registered trademark of Microsoft Corporation.

The WINDOWS-logo is a registered trademark <sup>(TM)</sup> of Microsoft Corporation.

## **Software License**

The software and the enclosed documentation are copyright-protected. By installing the software, you agree to the conditions of the licensing agreement.

## **Licensing Agreement**

SecuTech Solution Inc. (SecuTech for short) gives the buyer the simple, exclusive and non-transferable licensing right to use the software on one individual computer or networked computer system (LAN). Copying and any other form of reproduction of the software in full or in part as well as mixing and linking it with others is prohibited. The buyer is authorized to make one single copy of the software as backup. SecuTech reserves the right to change or improve the software without notice or to replace it with a new development. SecuTech is not obliged to inform the buyer of changes, improvements or new developments or to make these available to him. A legally binding promise of certain qualities is not given. SecuTech is not responsible for damage unless it is the result of deliberate action or negligence on the part of SecuTech or its aids and assistants. SecuTech accepts no responsibility of any kind for indirect, accompanying or subsequent damage.

## Contact Information

**HTTP:**        [www.eSecuTech.com](http://www.eSecuTech.com)

**E-Mail:**     [Sales@eSecuTech.com](mailto:Sales@eSecuTech.com)

Please Email any comments, suggestions or questions regarding this document or our products to us at: [Sales@eSecuTech.com](mailto:Sales@eSecuTech.com)

| Version | Date   |
|---------|--------|
| 1.0     | 2015.7 |

#### CE Attestation of Conformity



UniMate is in conformity with the protection requirements of CE Directives 89/336/EEC Amending Directive 92/31/EEC. UniMate satisfies the limits and verifying methods: EN55022/CISPR 22 Class B, EN55024: 1998.

#### FCC Standard



This device is in conformance with Part 15 of the FCC Rules and Regulation for Information Technology Equipment.

Operation of this product is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.



The equipment of UniMate is USB based.

#### Conformity to ISO 9001:2000



The Quality System of SecuTech Solution Inc., including its implementation, meets the requirements of the standard ISO 9001:2000

#### ROHS



All UniMate products are environmental friendly with ROHS certificates.

# Table of Contents

|   |    |
|---|----|
| Chapter 1: Console                                      | 1  |
| 1.1 Installation  | 1  |
| 1.2 Initialize a UniMate                                | 3  |
| 1.3 Manage pin  | 4  |
| 1.4 Manage certificates                                 | 6  |
| 1.5 Manage keys or keypairs                             | 14 |
| 1.6 Manage asymmetric keypairs                          | 17 |
| Chapter 2: Monitor tool                                 | 20 |
| 2.1 Installation  | 20 |
| 2.2 UniMate detection                                   | 22 |
| 2.3 Change Pin  | 22 |
| 2.4 Import certificate.                                 | 24 |
| 2.5 Register or unregister certificate.                 | 27 |
| 2.6 View certificate                                    | 33 |
| 2.7 Expiration reminder                                 | 35 |
| Chapter 3: Partition tool (only for UniMate drive)      | 36 |
| Chapter 4: Burner tool                                  | 38 |
| Chapter 5: Change language mode tool (For UniMate Flex) | 39 |

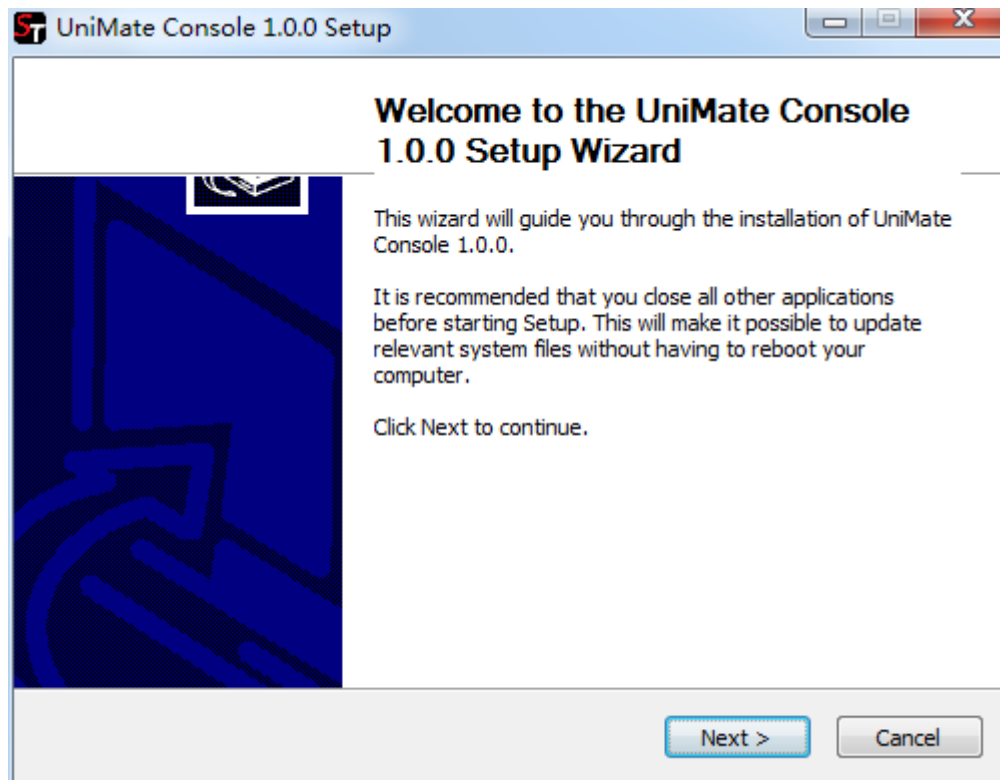
# Chapter 1: Console

UniMate Console is used to manage devices, initialize a UniMate as well as manage certificates and keys.

## 1.1 Installation

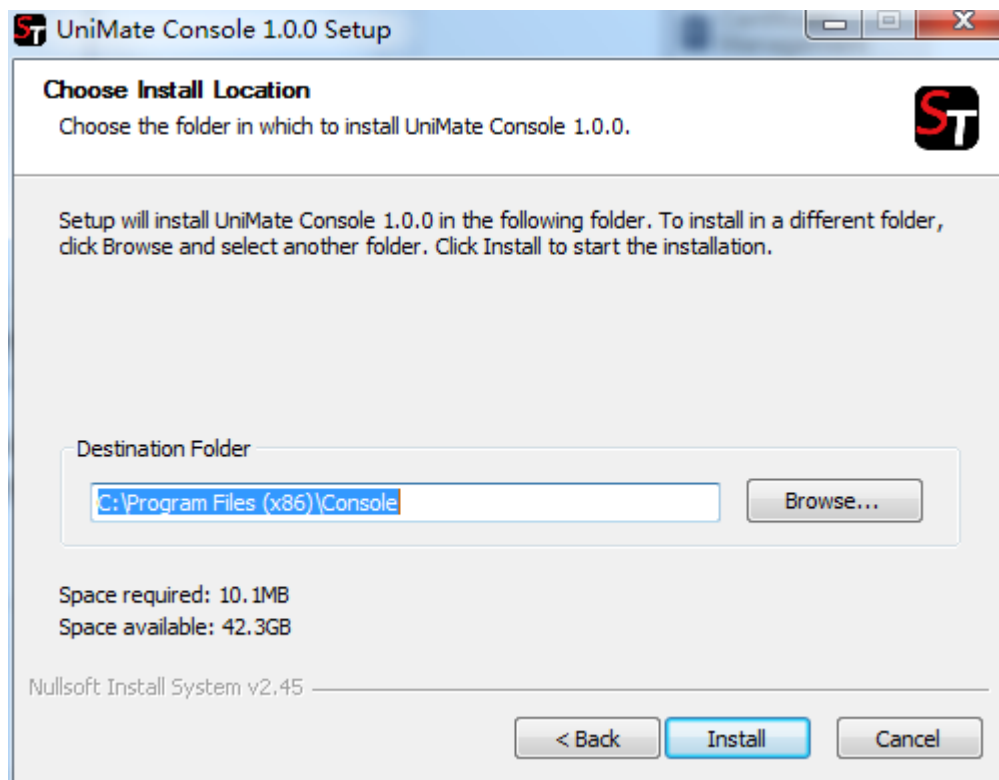
Console setup.exe can be found in the Utilities folder of UniMate SDK.

Run Console setup.exe.

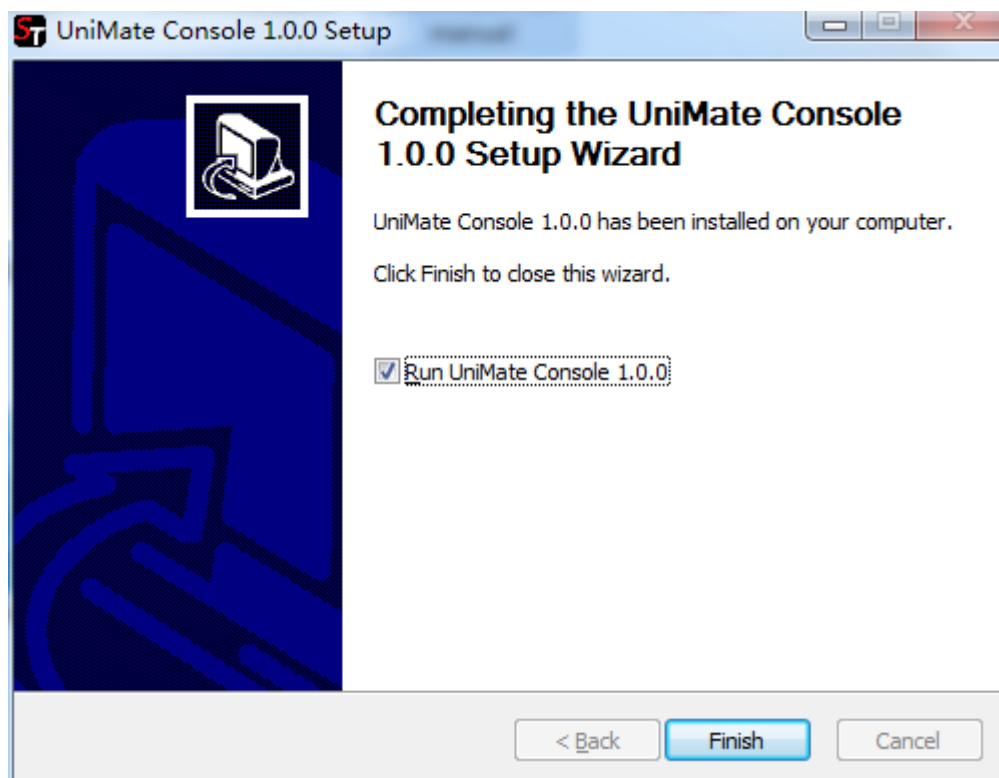


Click "Next"

Choose install location, and click “Install”.



At last, click “Finish” to close the setup wizard.

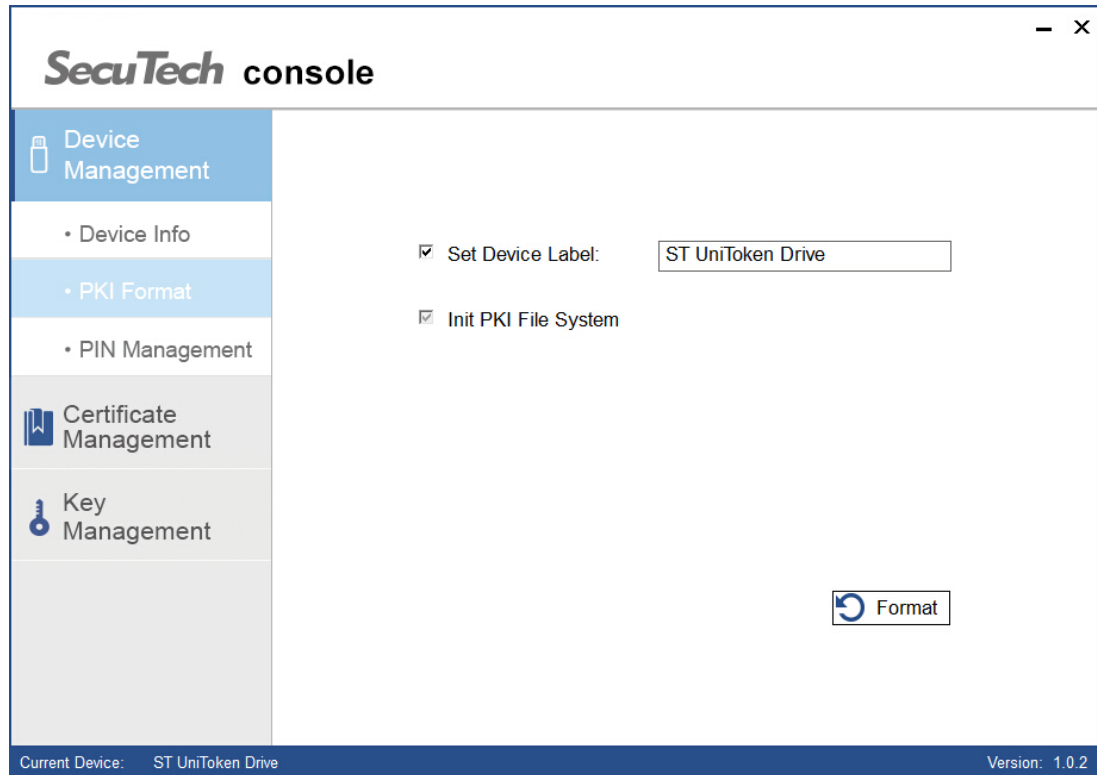


## 1.2 Initialize a UniMate

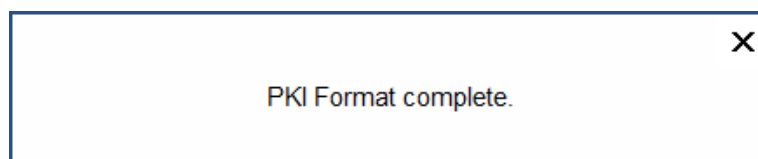
This operation will clean up all the certificates and keys on the PKI file system. Please proceed cautiously.

Click “PKI Format” on the menu bar.

Input a device name when a new name is required. Click “Format”.



Please verify the administrator’s access to this operation. The execution result will pop up later.



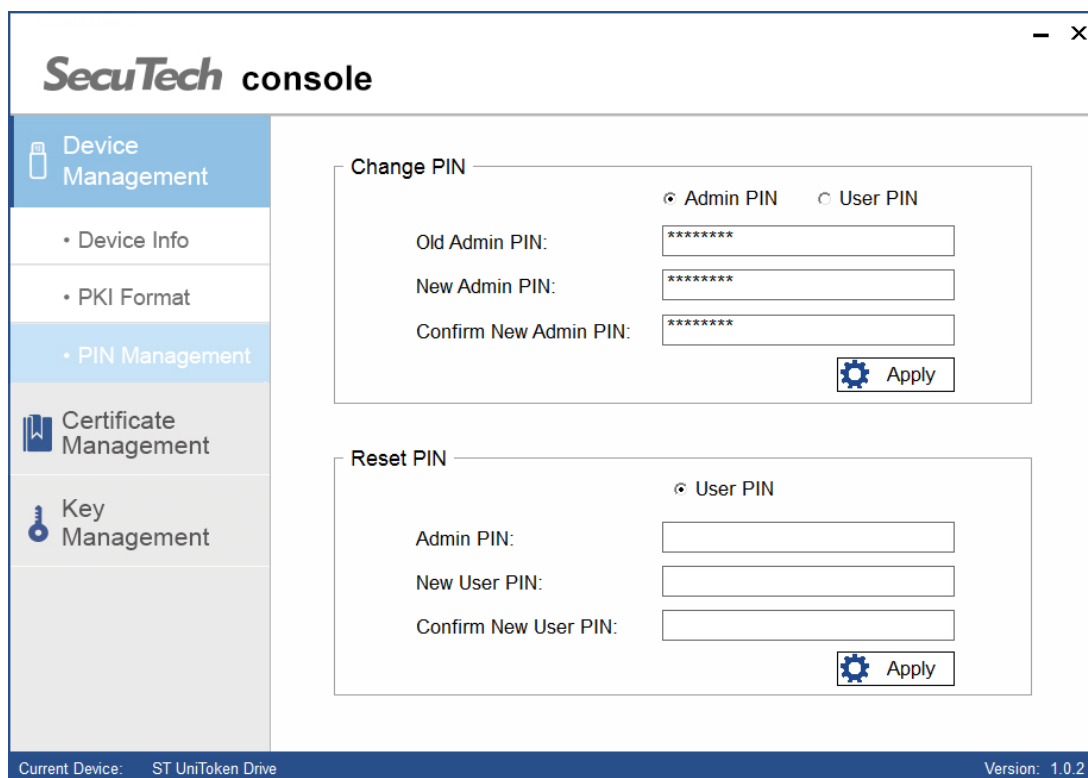


## 1.3 Manage pin

Pins should be between 8 and 24 characters long, If a user pin is locked, you could reset it with administrator's access.

Click "PIN Management" on the menu bar.

To change a pin, entering the old pin, creating a new pin and then re-entering it to confirm. Click "Apply".



The screenshot shows the SecuTech console interface. On the left is a sidebar menu with the following items: Device Management (selected), Device Info, PKI Format, PIN Management, Certificate Management, and Key Management. The main content area is titled "SecuTech console" and contains two sections: "Change PIN" and "Reset PIN".

**Change PIN Section:**

- Radio buttons for "Admin PIN" (selected) and "User PIN".
- Fields for "Old Admin PIN:", "New Admin PIN:", and "Confirm New Admin PIN:", each containing a masked input (\*\*\*\*\*).
- An "Apply" button with a gear icon.

**Reset PIN Section:**

- Radio button for "User PIN" (selected).
- Fields for "Admin PIN:", "New User PIN:", and "Confirm New User PIN:", each containing an empty input box.
- An "Apply" button with a gear icon.

At the bottom of the console, a status bar shows "Current Device: ST UniToken Drive" on the left and "Version: 1.0.2" on the right.

To reset a user pin, entering the admin pin, creating a new user pin and then re-entering it to confirm. Click “Apply”.

SecuTech console

Device Management

• Device Info

• PKI Format

• PIN Management

Certificate Management

Key Management

Change PIN

Admin PIN

User PIN

Old Admin PIN:

New Admin PIN:

Confirm New Admin PIN:

Apply

Reset PIN

User PIN

Admin PIN:

\*\*\*\*\*

New User PIN:

\*\*\*\*\*

Confirm New User PIN:

\*\*\*\*\*

Apply

Current Device: ST UniToken Drive

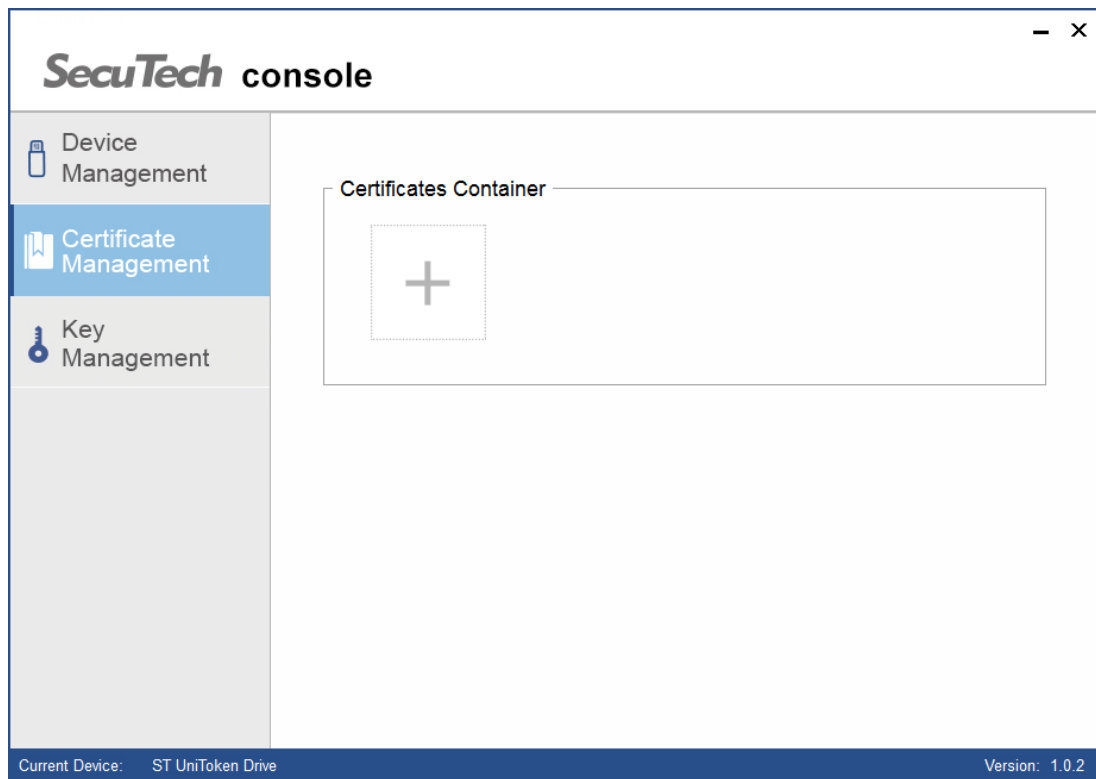
Version: 1.0.2

## 1.4 Manage certificates

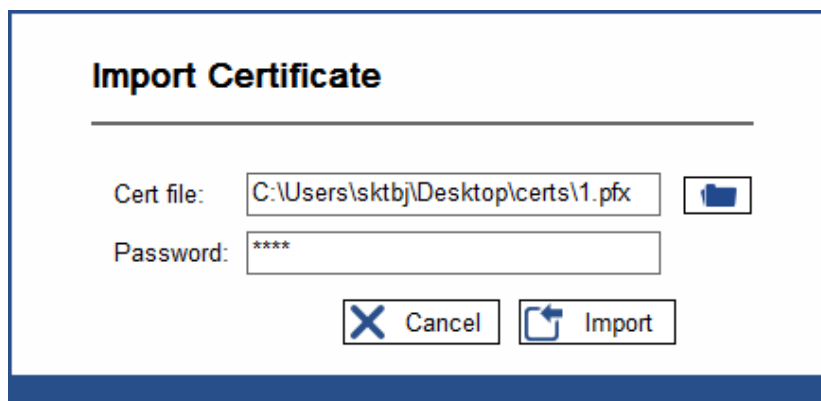
Certificates container displays the existing certificates. Each UniMate can carry a maximum of 8 certificates or asymmetric keypairs.

### 1.4.1 Importing certificates

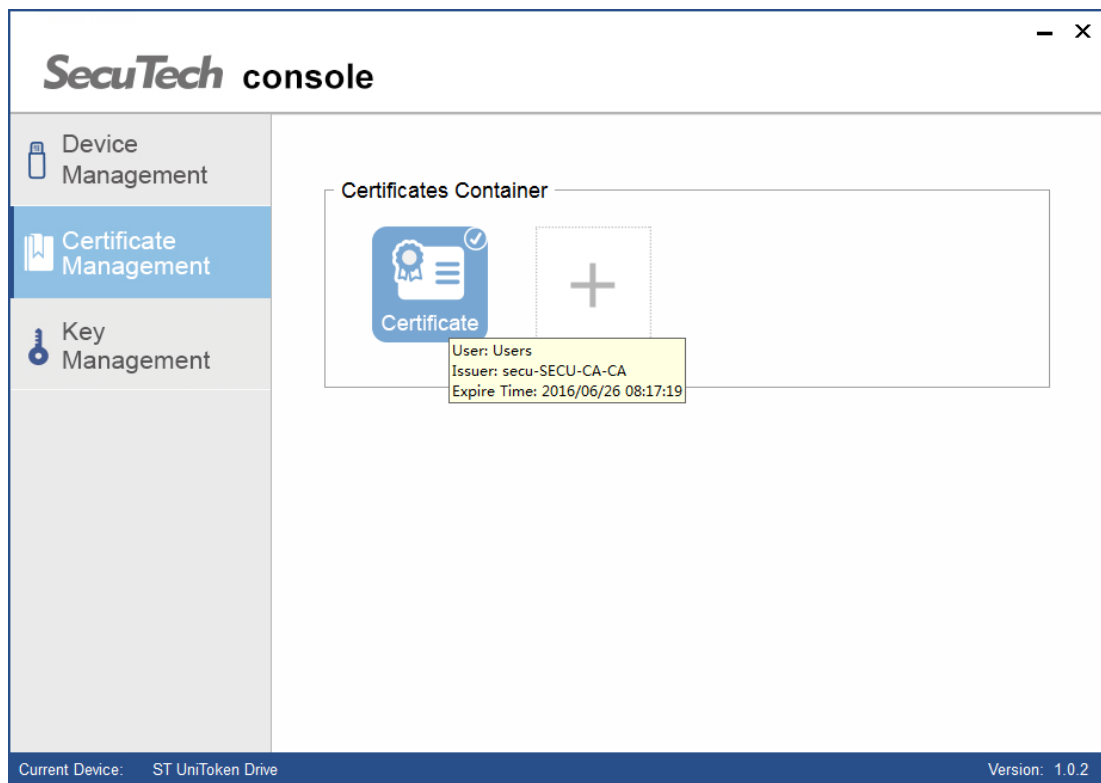
Click “Certificates Management” on the menu bar. Click on the “+” button.



Login with the user pin if you haven't got permission. Select a certificate file (.pfx or .p12) and input the password. Click “Import”.

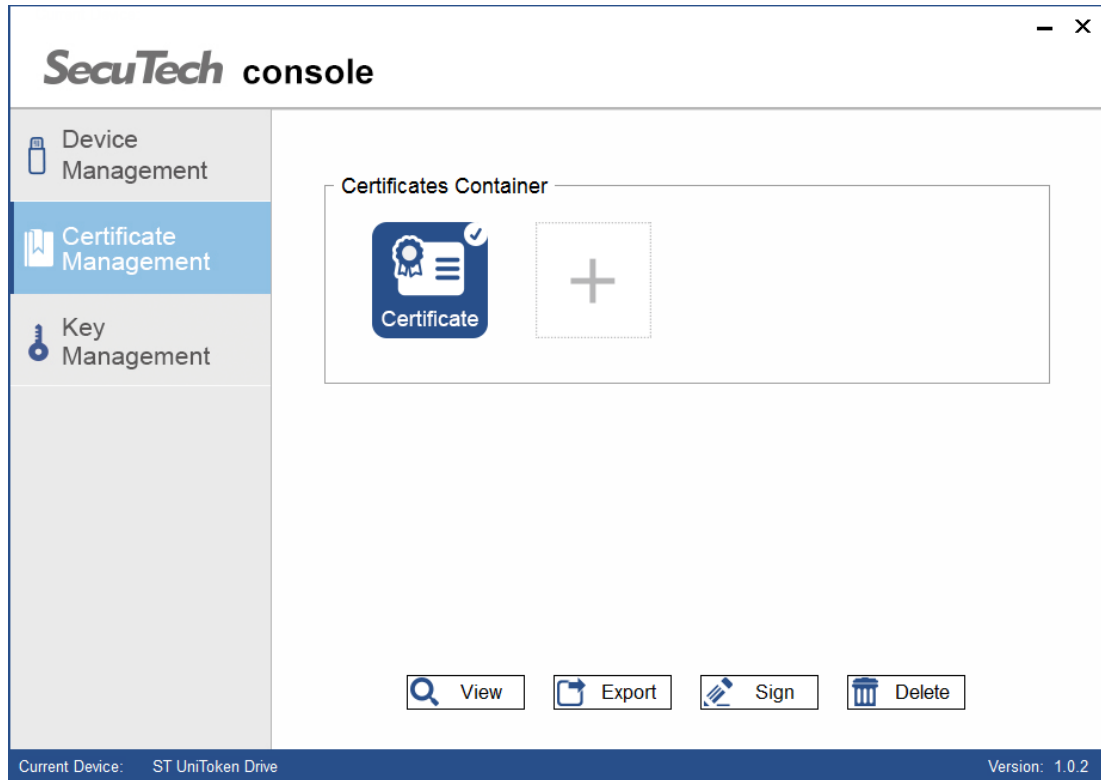


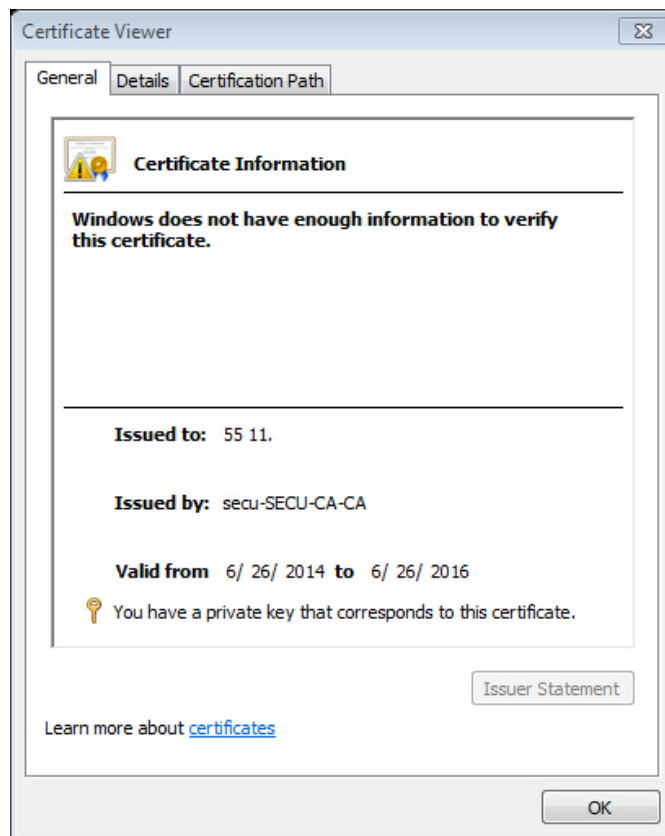
Now the certificate has been imported. Hover the mouse over it, and the certificate information will be listed as shown below.



### 1.4.2 View certificates

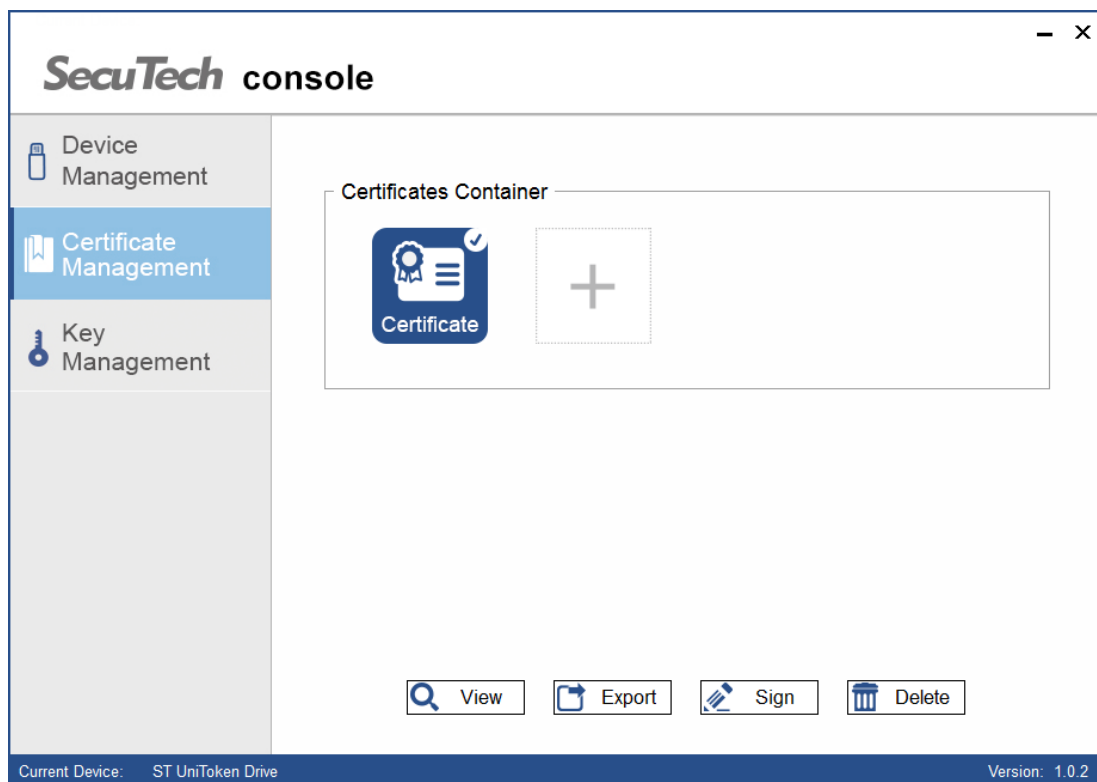
To view a certificate, click to select a certificate. Click “View” to see the certificate details.



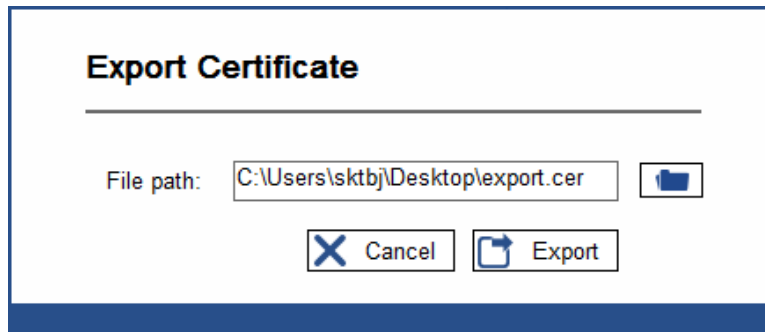


### 1.4.3 Export certificate

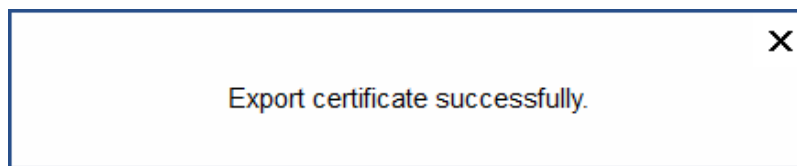
To export a certificate, click to select a certificate. Click “Export”.



Select a file path and click “Export”.



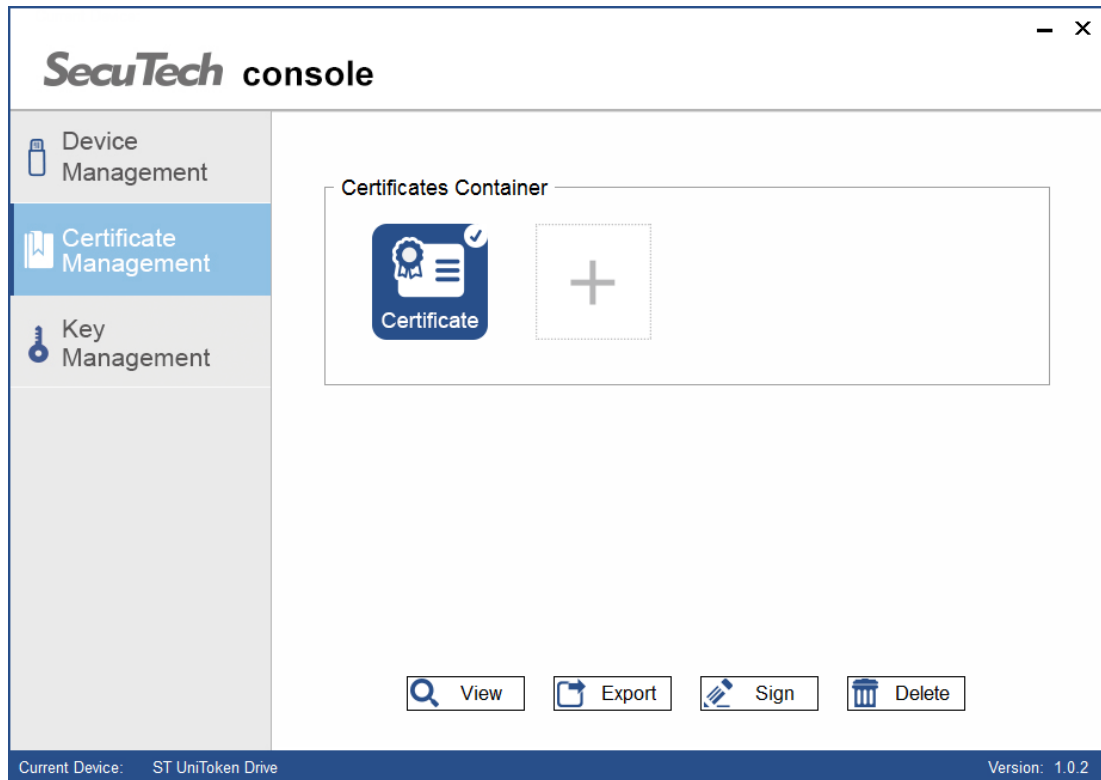
The execution result will pop up later.



#### 1.4.4 Signing with certificate

To sign with a private key or verify the public key of a certificate.

Click to select a certificate. Click “Sign”.





To sign with private key.

Choose “Sign” and select the mode. Input the data to be signed in hexadecimal format. For example, you could enter 0d0a, which consists of four hexadecimal digits (two bytes) and represents 0x0d0a. At last, click “Sign”, the signed data will be displayed on the right side.

### Certificate Operation


---


Action:

Mode:

Data to be signed: (Hex)

Signed data:

 Cancel

 Sign

To verify with public key, choose “Verify” and select the mode. Input the data to be signed as well as the signed data. Click “Verify”.

### Certificate Operation

---

Action:

Mode:

Data to be signed: (Hex)

0d0a

Signed data:

b1d1a0cbcd21253ed79e5405  
96ff1cdd864425012a25dcdd  
73a06baf46427a969178b255e  
1b99c2166762a5eee387a0bc  
b79bdd333f8e5e4fe0710c09c  
ba008618cc9e94ef4230864d9  
d758d99496d4995f4c9ecef77  
5e3277b6f2c81c3ec3c8ca7d4

The execution result will pop up later.

×

Verify successfully.

#### 1.4.5 Deleting certificates

Click to select a certificate. Click “Delete”.

### Delete Certificate

---

Are you sure to delete this certificate?

☒ Yes
☐ No

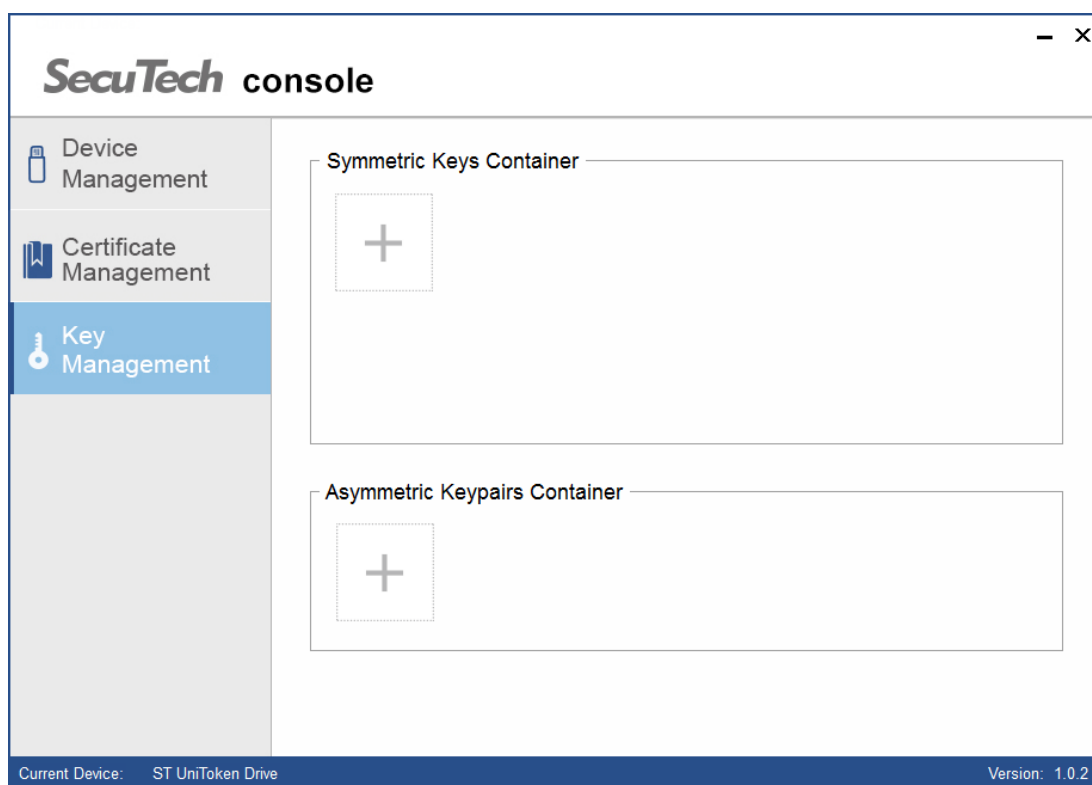
Click “Yes” to complete delete operation.

## 1.5 Manage keys or keypairs

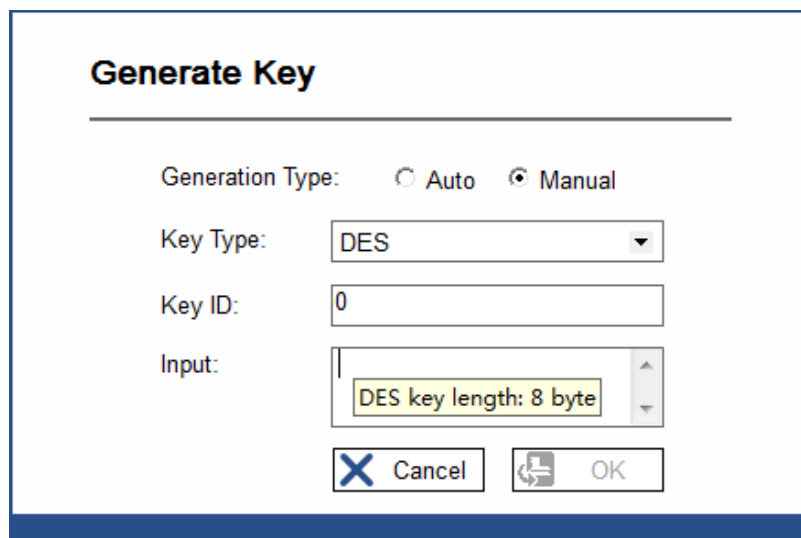
Existing keys and keypairs are shown in the symmetric keys and asymmetric keypairs container respectively. Each UniMate can carry a maximum of 12 symmetric key and a maximum of 4 certificates or asymmetric keypairs.

### 1.5.1 Key generation

Click “Key Management” on the menu bar. Login with user pin if you haven't got the permission. Next, click on “+” button.



Click “Auto” if you want to generate a key automatically. If you click “Manual”, you have to input the keys manually. Move the mouse to the edit box, it will shows the tip. Next, please input a key ID as a unique number of the key. At last, click “OK”.



**Generate Key**

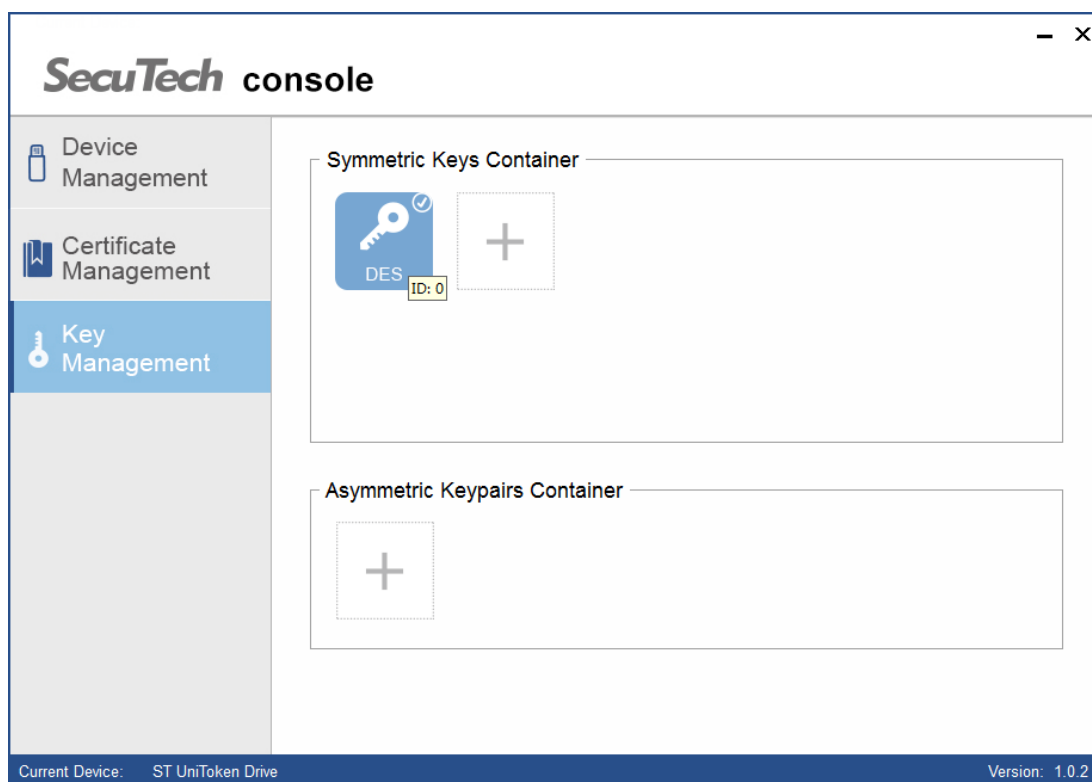
Generation Type: ☐ Auto ☒ Manual

Key Type:

Key ID:

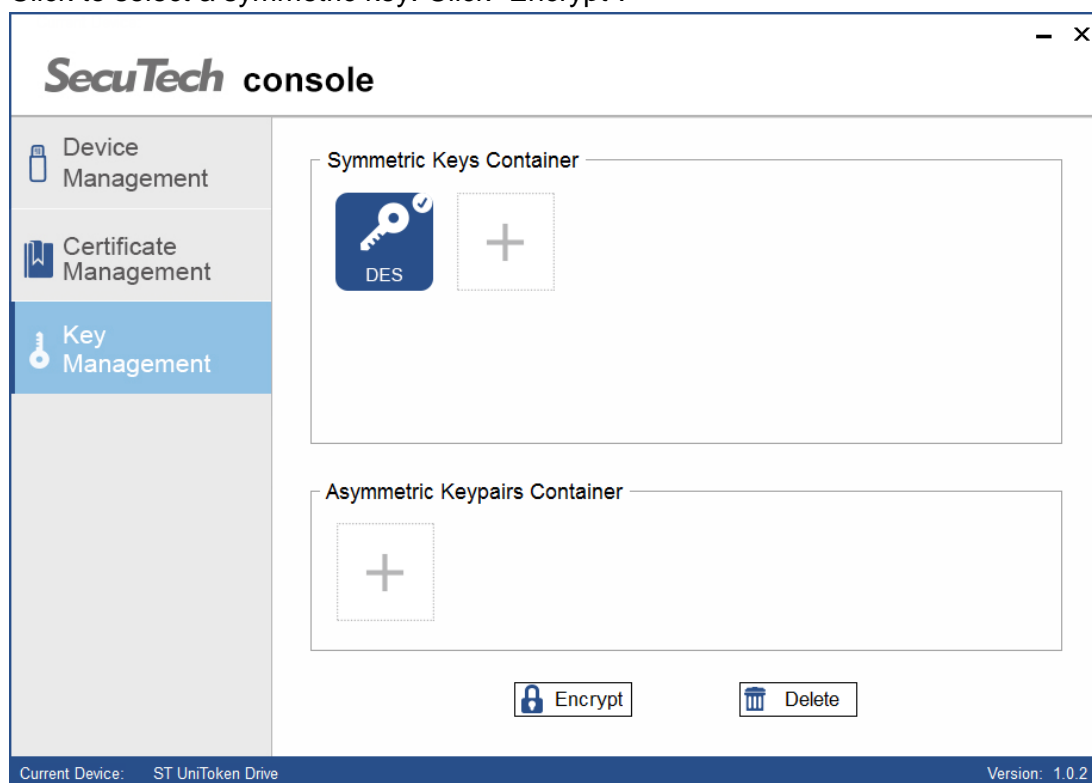
Input:

Now, the symmetric key has been generated. Move the mouse to it, the key ID will be displayed as shown below.



### 1.5.2 Encrypt or decrypt with a symmetric key.

Click to select a symmetric key. Click “Encrypt”.



Select the action to be performed and the mode as well. Please input “iv” when CBC or CBC\_PAD has been chosen. Next, input the data to be operated. Click “Encrypt” or “Decrypt”, the output data will display on the right side.

## Key Operation

Action:

Encrypt

Key type:

DES

Key ID:

0

Mode:

ECB

iv:

Input data: (Hex)

DES plain group length: 8 byte

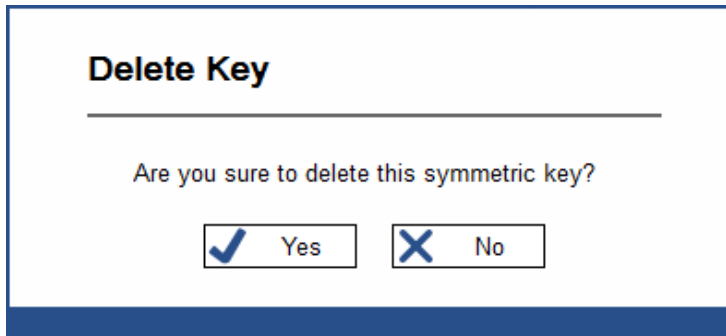
Output data:

Cancel

Encrypt

### 1.5.3 Delete a symmetric key.

Click to select a symmetric key, then click “Delete”.

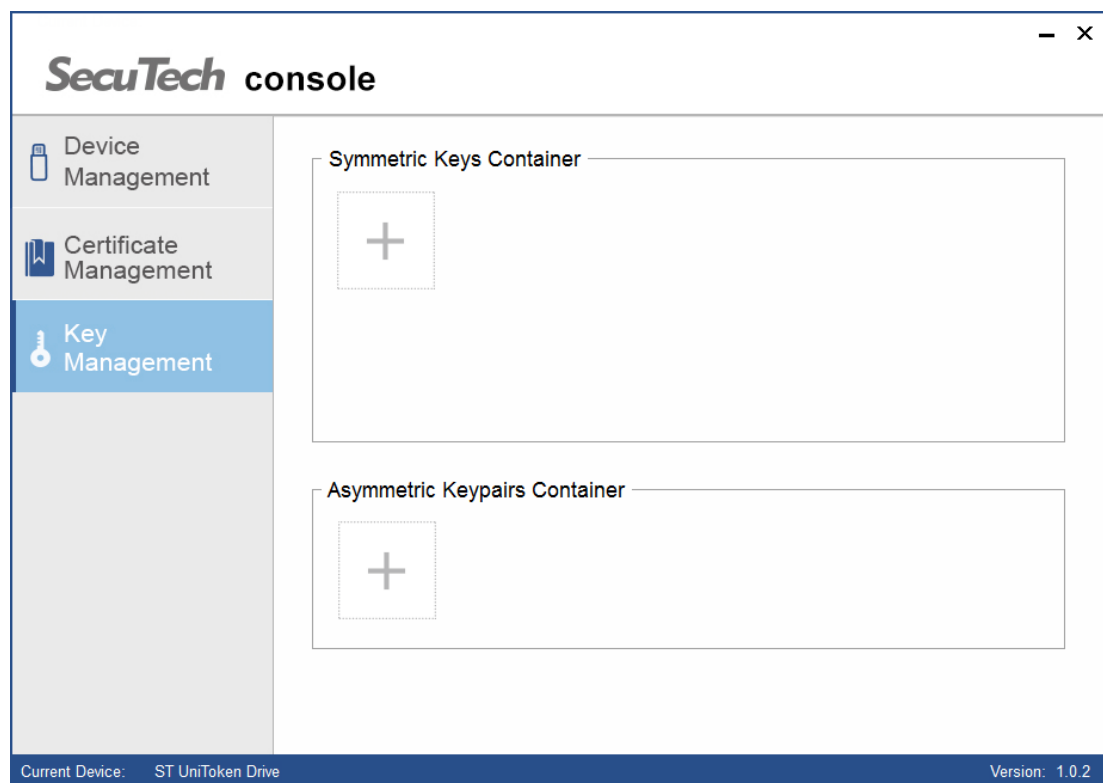


Click “Yes” to complete delete operation.

## 1.6 Manage asymmetric keypairs

### 1.6.1 Generate a keypair

Click “Key Management” on the menu bar. Login with user pin if you haven’t got the permission. Next, click on “+” button.



Select a keypair type and input a keypair ID as a unique number. Click “Generate”.

### Generate Keypair

---

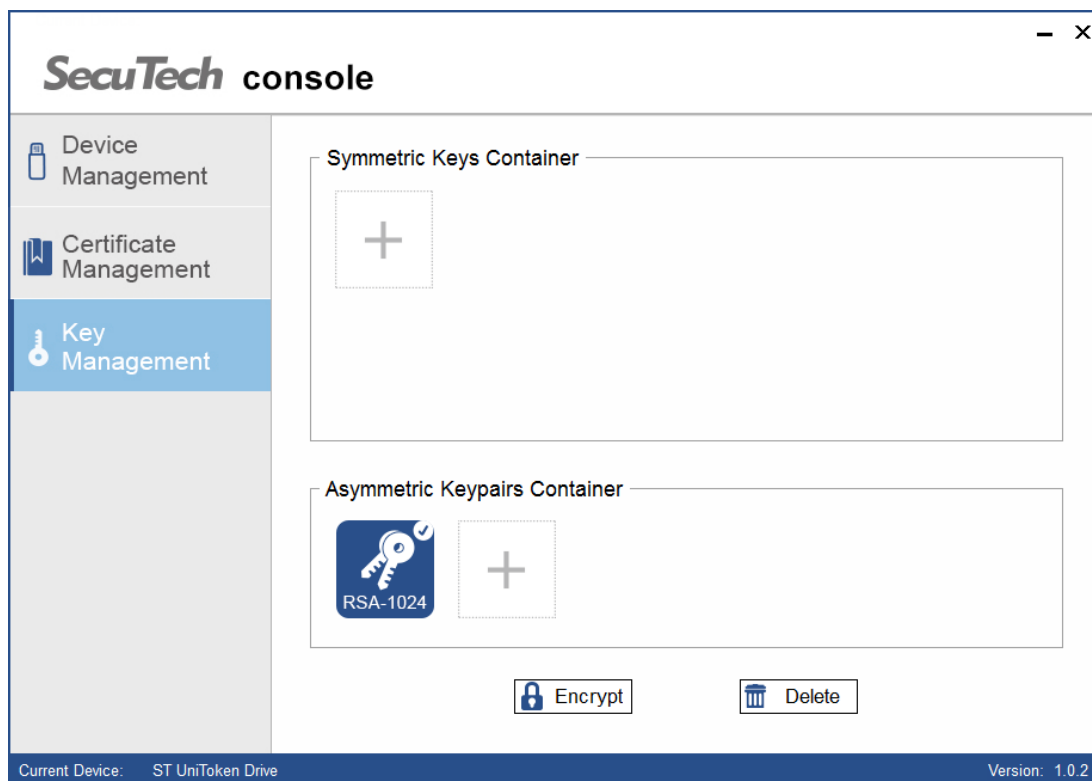
Keypair Type: RSA-1024

Keypair ID: 0

✕ Cancel
📄 Generate

### 1.6.2 *Encrypt, decrypt, sign or verify with an asymmetric keypair.*

Click to select an asymmetric keypair. Click “Encrypt”.



Select the action to be performed.. If you click “Private-key Sign” or “Public-key Verify”, you have to choose the mode. Next, input the data to be operated.

Click “Encrypt”, “Decrypt” or “Sign”, the output data will display on the right side.

If you select “Public-key Verify”, you should input the data to be signed as well as the signed data. Click “Verify”. The execution result will pop up later.

### Keypair Operation

---

Action:

Private-Key Sign ▼

Key ID:

0

Key type:

RSA-1024

Mode:

MD5 ▼

Data to be signed: (Hex)

Signed data:

✕ Cancel

✓ Sign

### 1.6.3 Delete an asymmetric keypair.

Click to select an asymmetric keypair. Click “Delete”.

### Delete Keypair

---

Are you sure to delete this asymmetric keypair?

✓ Yes

✕ No

Click “Yes” to complete delete operation.

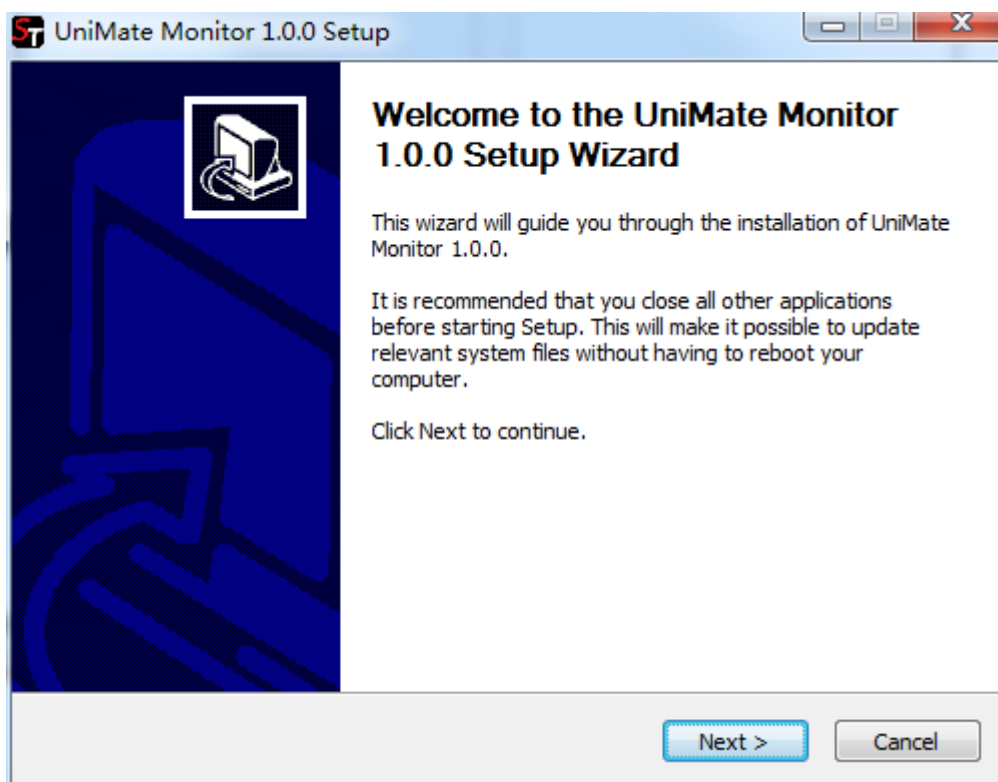


## Chapter 2: Monitor tool

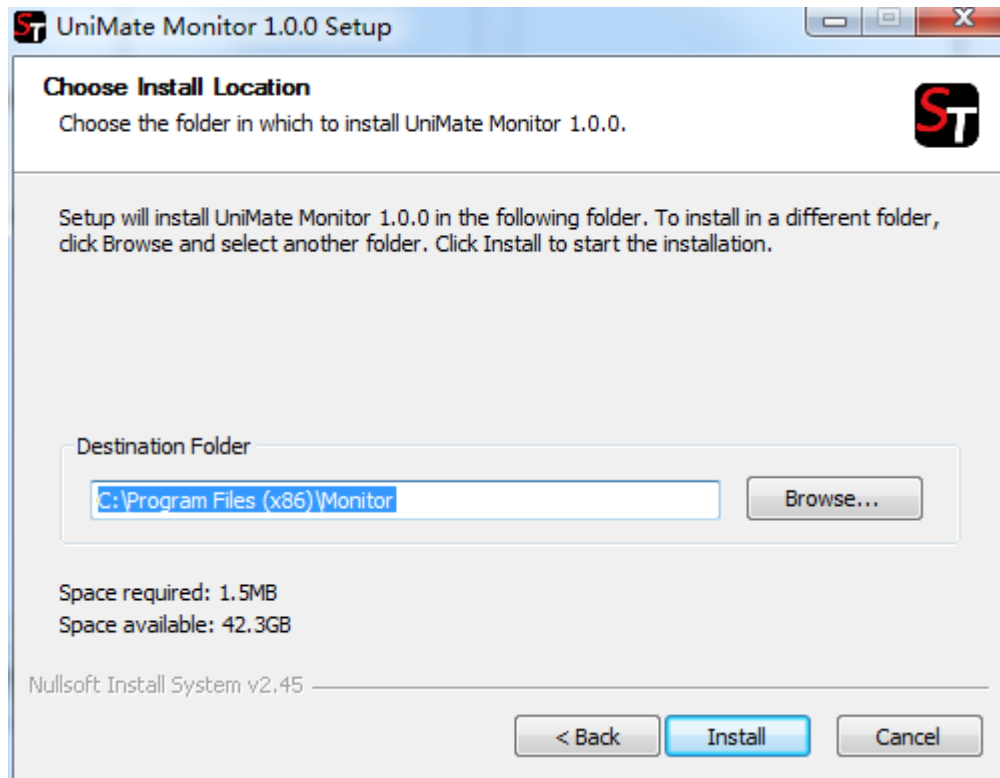
UniMate Monitor is used to view the detailed information of certificates imported into the UniMate and register or delete certificates. It also provides a way to check UniMate information and to change User PIN.

### 2.1 Installation

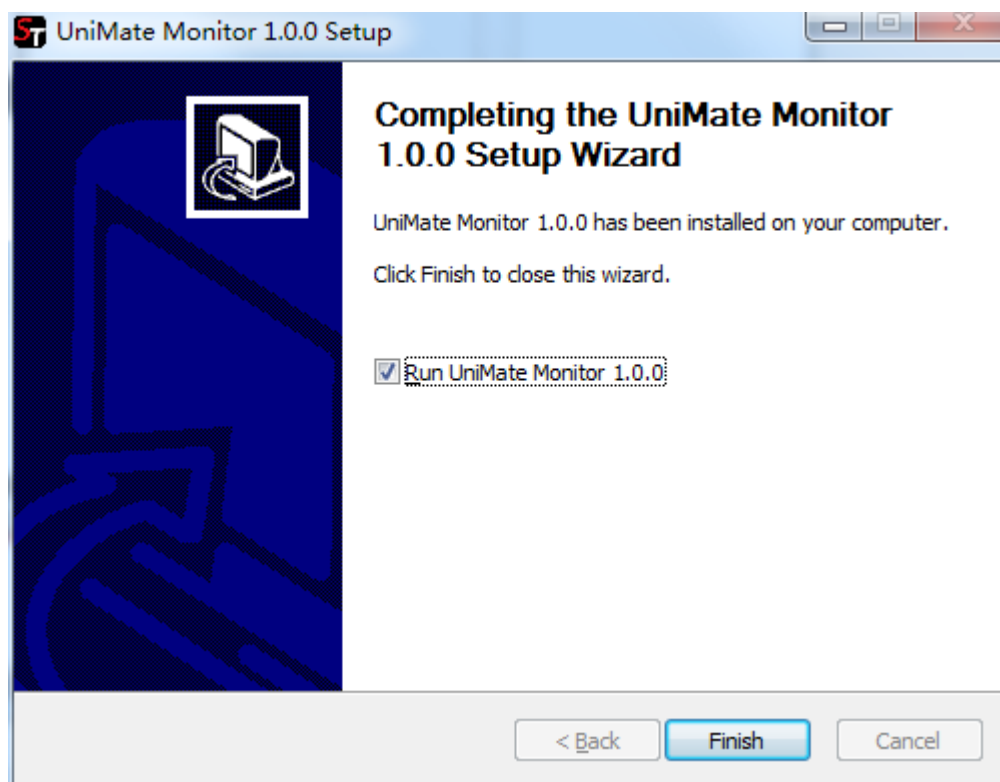
Run Monitor setup.exe.



Click "next"



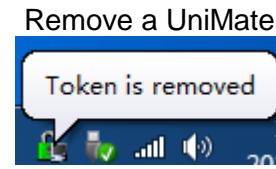
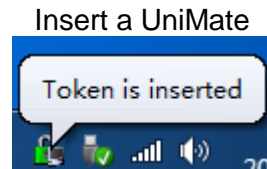
Choose install location, and click “Install”.



Click “Finish” to close the setup wizard.

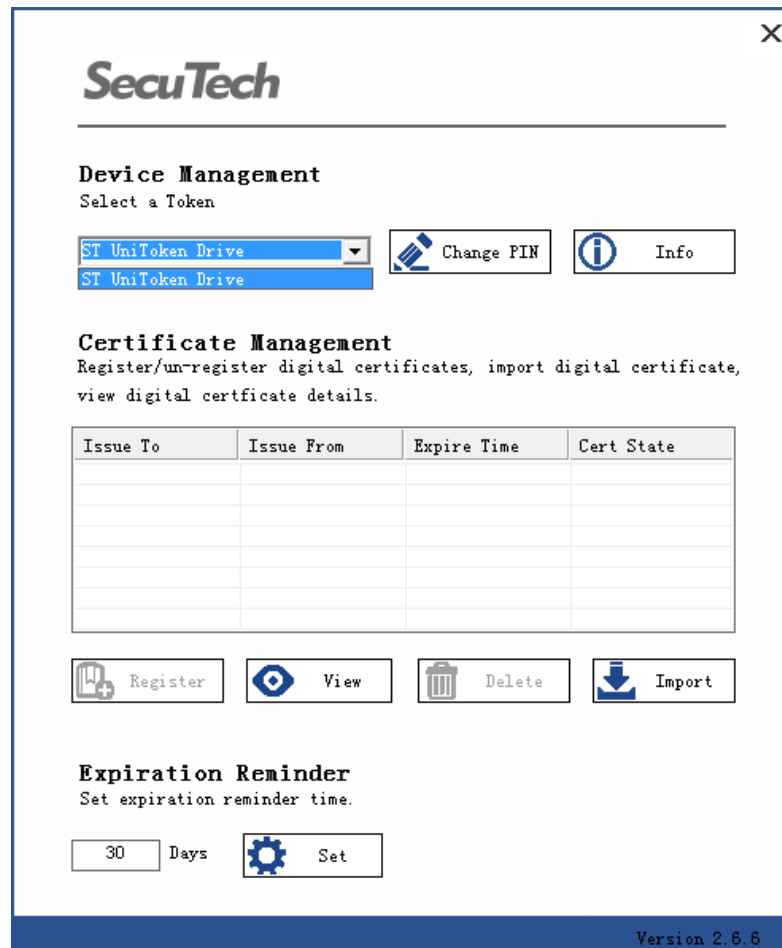
## 2.2 UniMate detection

Once the Monitor tool is installed, a new icon appears in the system tray, it will inform you when a UniMate is detected like so:

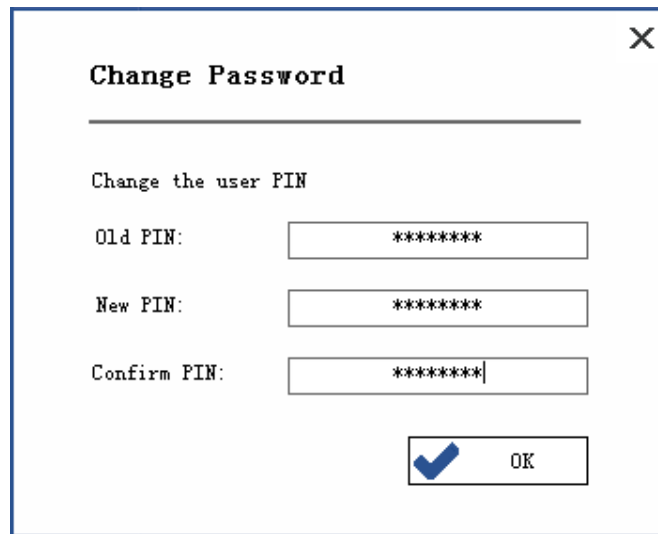


## 2.3 Change Pin

Insert a UniMate and select a target device. Click “Change PIN”.

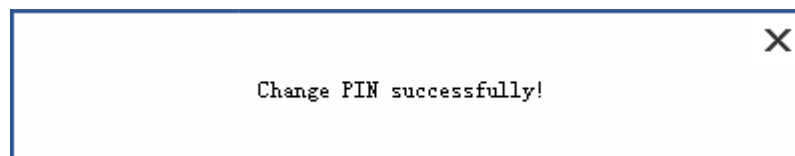


To change a pin, entering the old pin, creating a new pin and then re-entering it to confirm. Click "OK".



A dialog box titled "Change Password" with a close button (X) in the top right corner. Below the title is a horizontal line. The text "Change the user PIN" is displayed. There are three input fields: "Old PIN:" with "\*\*\*\*\*", "New PIN:" with "\*\*\*\*\*", and "Confirm PIN:" with "\*\*\*\*\*|". A blue checkmark icon is to the left of the "OK" button.

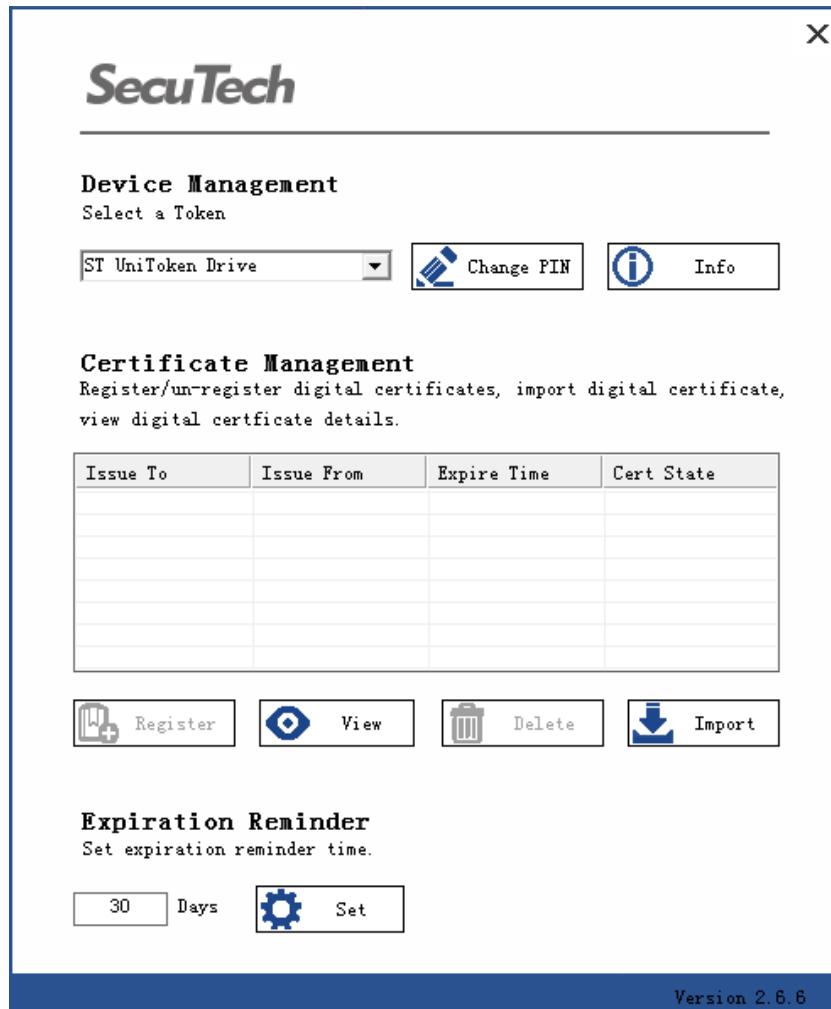
The execution result will pop up.



A dialog box with a close button (X) in the top right corner. The text "Change PIN successfully!" is centered.

## 2.4 Import certificate.



Click "Import".



**SecuTech**





---

**Device Management**  
Select a Token


ST UniToken Drive  Change PIN  Info

**Certificate Management**  
Register/un-register digital certificates, import digital certificate, view digital certificate details.

| Issue To | Issue From | Expire Time | Cert State |
|----------|------------|-------------|------------|
|          |            |             |            |
|          |            |             |            |
|          |            |             |            |
|          |            |             |            |
|          |            |             |            |
|          |            |             |            |

 Register  View  Delete  Import

**Expiration Reminder**  
Set expiration reminder time.

30 Days  Set

Version 2.6.6

Login in with user pin if you haven't got permission.



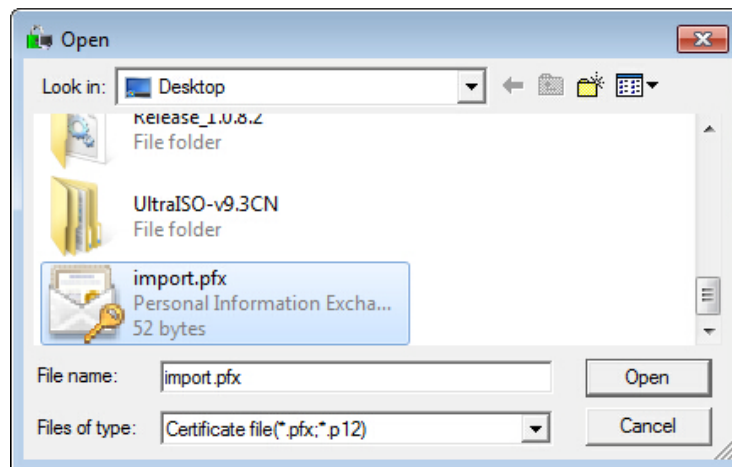
**User Login**

---

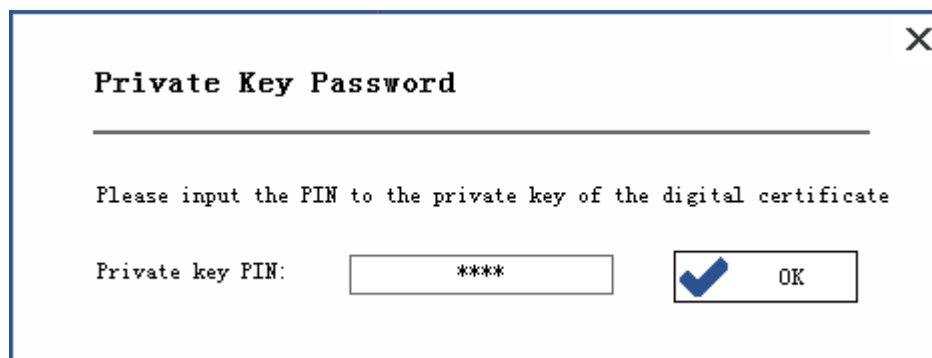
Login the UniToken to operate the certificate.

User PWD:   Login

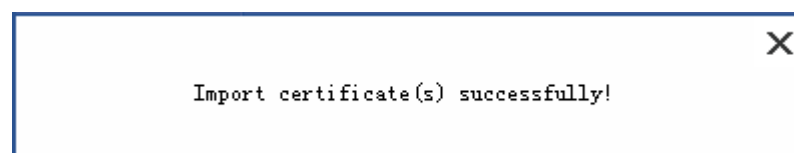
Select a certificate file(.pfx or .p12).



Input the password of the certificate.




The execution result will pop up.



The certificate is now displayed in the list.


X




---

**Device Management**  
 Select a Token


ST UniToken Drive ▼


 Change PIN


 Info


**Certificate Management**  
 Register/un-register digital certificates, import digital certificate, view digital certificate details.

| Issue To | Issue From      | Expire Time     | Cert State      |
|----------|-----------------|-----------------|-----------------|
| Users    | secu-SECU-CA-CA | 2016/06/26 1... | Register Suc... |
|          |                 |                 |                 |
|          |                 |                 |                 |
|          |                 |                 |                 |
|          |                 |                 |                 |

 Register

 View


 Delete

 Import

**Expiration Reminder**  
 Set expiration reminder time.

30

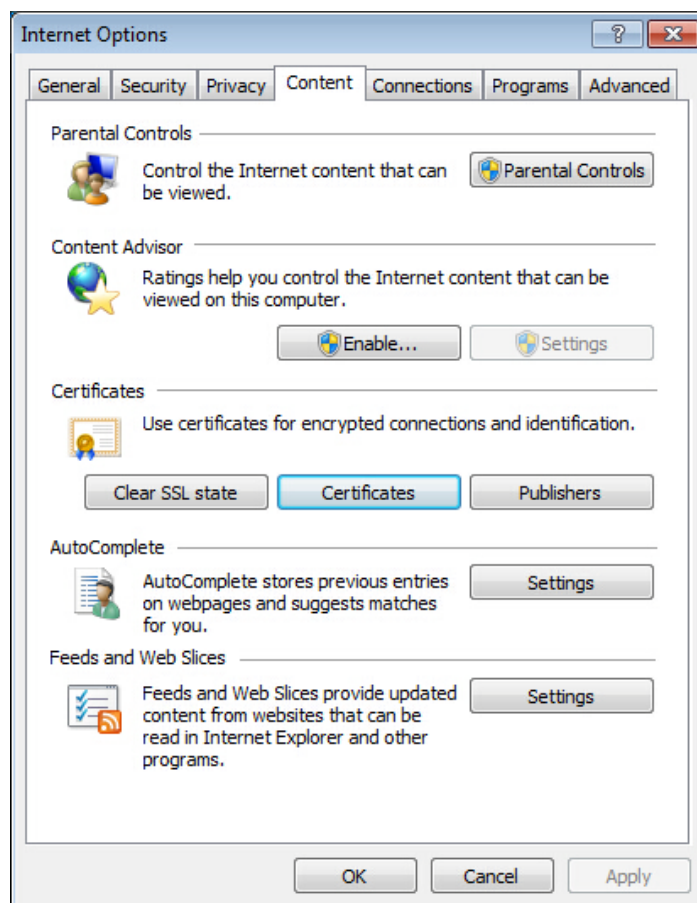
Days

 Set

Version 2.6.6

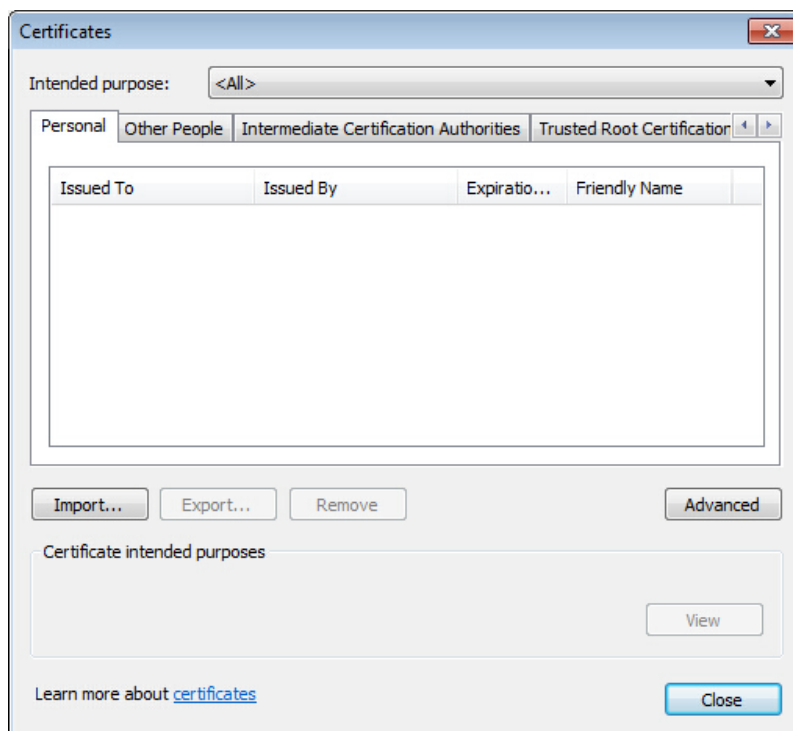
## 2.5 Register or unregister certificate.

In IE -- Tools -- Internet Options – Content – Certificates check the registered certificates.







As an example, there's no certificate yet.



To register a certificate. Select a certificate and click "Register".







---

**Device Management**  
Select a Token


ST UniToken Drive


 Change PIN


 Info


**Certificate Management**  
Register/un-register digital certificates, import digital certificate, view digital certificate details.

| Issue To | Issue From      | Expire Time     | Cert State   |
|----------|-----------------|-----------------|--------------|
| Users    | secu-SECU-CA-CA | 2016/06/26 1... | Not Register |
|          |                 |                 |              |
|          |                 |                 |              |
|          |                 |                 |              |
|          |                 |                 |              |

 Register

 View


 Delete

 Import

**Expiration Reminder**  
Set expiration reminder time.


30

Days

 Set

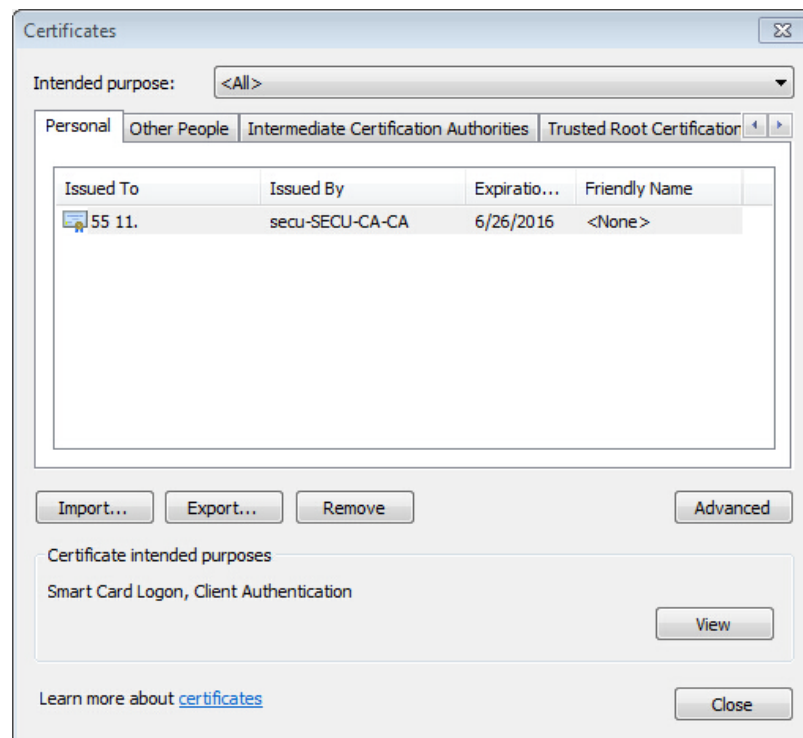
Version 2.6.6

The certificate is registered.



The certificate is registered successfully!

Go back to the IE – Tools – Internet Options – Content – Certificates, the registered certificate is now displayed in the list.



To unregister a certificate. Select a certificate and click “Un-Register”

X


## SecuTech


---

### Device Management

Select a Token

ST UniToken Drive

 Change PIN


 Info


  


### Certificate Management


Register/un-register digital certificates, import digital certificate, view digital certificate details.

| Issue To | Issue From      | Expire Time     | Cert State      |
|----------|-----------------|-----------------|-----------------|
| Users    | secu-SECU-CA-CA | 2016/06/26 1... | Register Suc... |
|          |                 |                 |                 |
|          |                 |                 |                 |
|          |                 |                 |                 |
|          |                 |                 |                 |
|          |                 |                 |                 |

 Un-Register

 View

 Delete

 Import


  

### Expiration Reminder

Set expiration reminder time.

30

Days

 Set

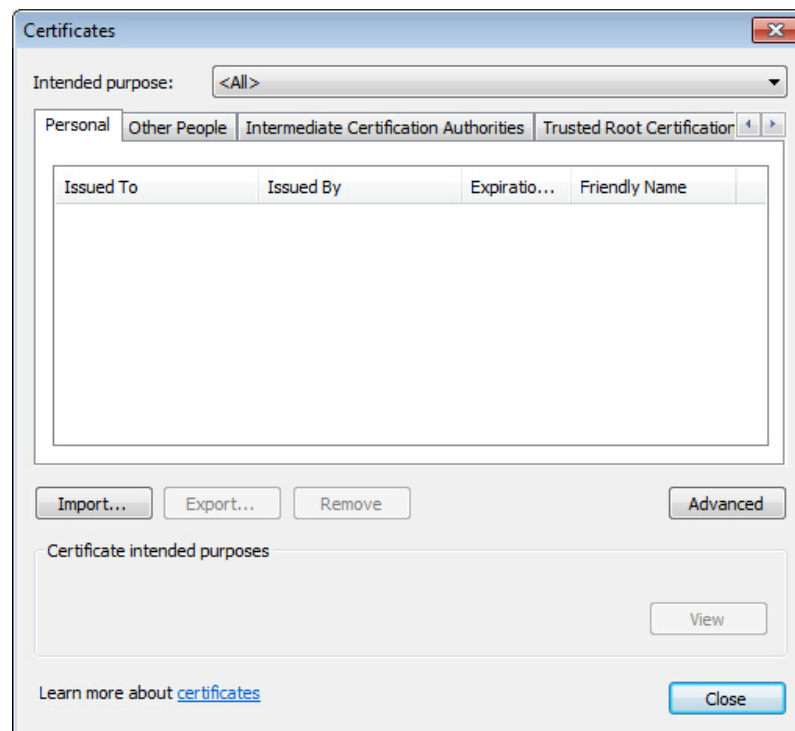
Version 2.6.6

The certificate is unregistered.

X


The certificate is un-registered successfully!


Back to the IE – Tools – Internet Options – Content – Certificates, the registered certificate has been removed.



## 2.6 View certificate

Select a certificate.







---

**Device Management**  
 Select a Token


ST UniToken Drive


 Change PIN


 Info


**Certificate Management**  
 Register/un-register digital certificates, import digital certificate, view digital certificate details.

| Issue To | Issue From      | Expire Time     | Cert State      |
|----------|-----------------|-----------------|-----------------|
| Users    | secu-SECU-CA-CA | 2016/06/26 1... | Register Suc... |
|          |                 |                 |                 |
|          |                 |                 |                 |
|          |                 |                 |                 |
|          |                 |                 |                 |
|          |                 |                 |                 |

 Un-Register

 View


 Delete

 Import

**Expiration Reminder**  
 Set expiration reminder time.

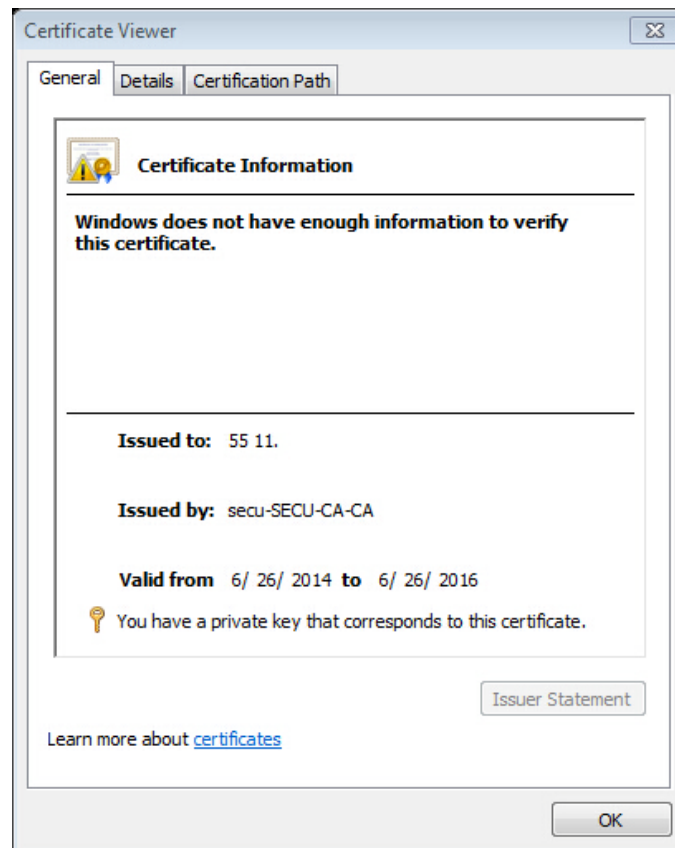
30

Days

 Set

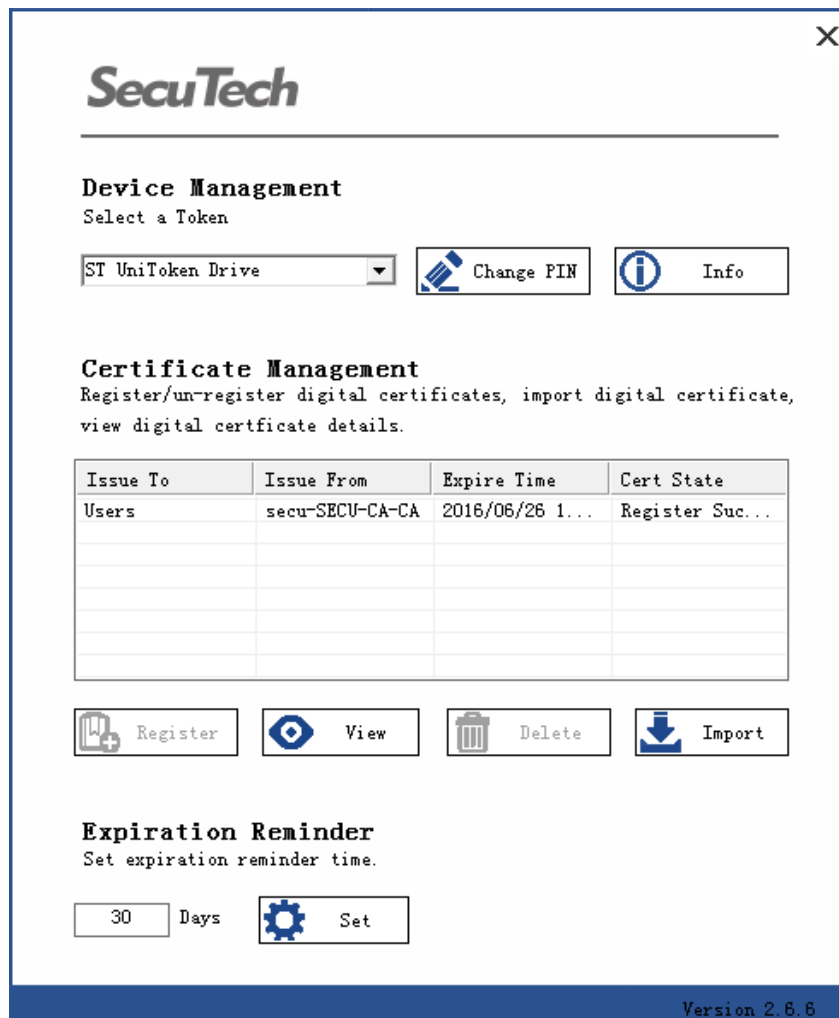
Version 2.6.6

Click “View” to see the detailed certificate.

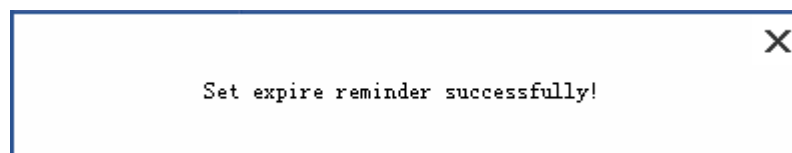


## 2.7 Expiration reminder

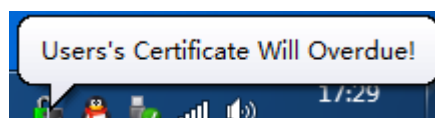
Set expiration reminder time.



Click "Set".



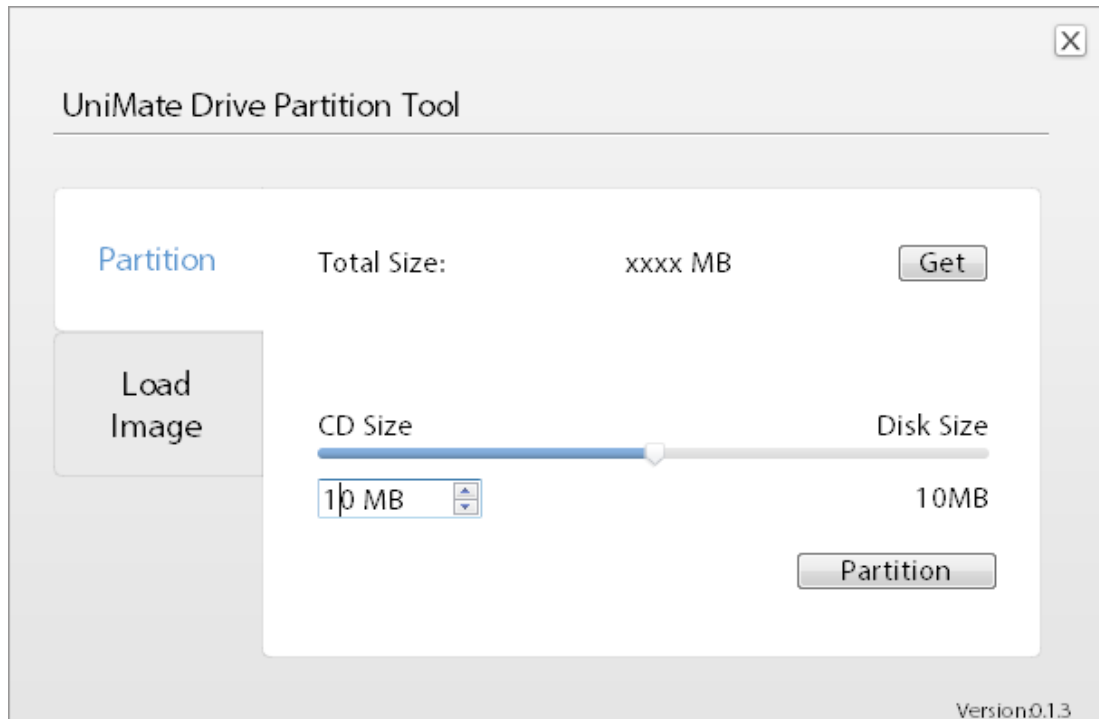
Click "Set". When the time is getting close to the expiration date, bubble tips will show up.





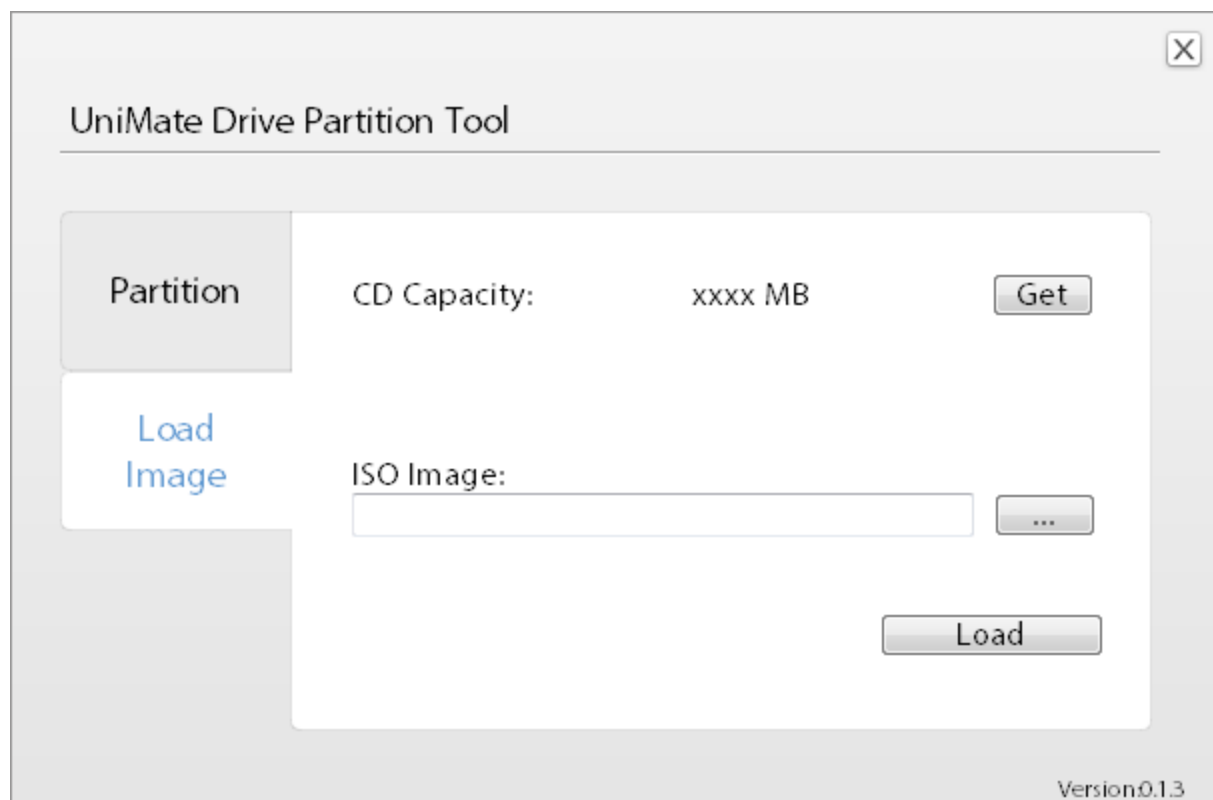
## Chapter 3: Partition tool (only for UniMate drive)

UniMate Drive Partition tool allows developer to set partitions, and to upload an ISO image to the Drive's CD-ROM.



Click “Get”, then you’ll get the total size of the Drive.

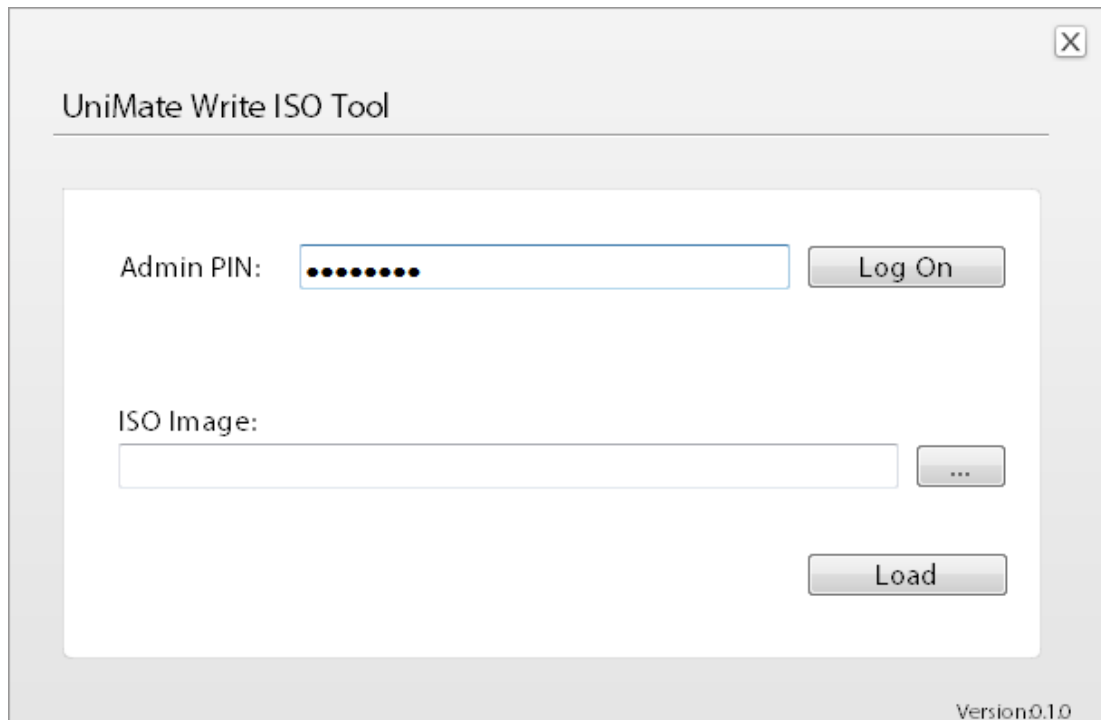
You can set partition sizes as you wish, then click “Partition” to perform the resize operation.



Clicking on “LoadImage”, you can load an ISO image to the Drive’s CD-ROM partition

## Chapter 4: WriteISO tool

UniMate WriteISO is a tool for writing ISO image to UniKey dongles.



## Chapter 5: Change language mode tool (For UniMate Flex)

UniMate change language mode tool is a tool for changing language mode for UniMate Flex.



## Follow us!


[Twitter](#)

[Facebook](#)

[Youtube](#)

[Linked in](#)


## About SecuTech

SecuTech Solution Inc. is a company specializing in data protection and strong authentication, providing total customer satisfaction in security systems & services for banks, financial institutions & other industries. Having extensive and in-depth experience within the information security market, SecuTech has drawn upon this experience to utilize today's cutting-edge technologies, enables enterprises, financial institutions, and government to safely adopt the economic benefits of mobile and cloud computing that are effective against increasingly sophisticated cyber attacks.

# SecuTech

[www.eSecuTech.com](http://www.eSecuTech.com) SecuTech Solution Inc.

### North America

1250 Boulevard René-Lévesque Ouest, #2200,  
Montreal, QC, H3B 4W8,  
Canada  
T: +1 -888-259-5825  
F: +1 -888-259-5825 ext.0  
E: [INFO@eSecuTech.com](mailto:INFO@eSecuTech.com)

### China

Level 12, #67 Bei Si Huan  
Xi Lu,  
Beijing, China, 100080  
T: +8610-8288 8834  
F: +8610-8288 8834  
E: [CN@eSecuTech.com](mailto:CN@eSecuTech.com)

### APAC

Suite 5.14, 32 Delhi Rd,  
North Ryde,  
NSW, 2113, Australia  
T: 00612-9888 6185  
F: 00612-9888 6185  
E: [AUS@eSecuTech.com](mailto:AUS@eSecuTech.com)

### EMEA

4 Cours Bayard 69002  
Lyon, France  
T: +33-042-600-2810  
F: +33-042-600-2810  
M: +33-060-939 6463  
E: [Europe@eSecuTech.com](mailto:Europe@eSecuTech.com)

©Copyright 2012 SecuTech Solution Inc. All rights reserved. Reproduction in whole or in part without written permission from SecuTech is prohibited. SecuTech UniMate and the SecuTech logo are trademarks of SecuTech Inc. Windows and all other trademarks are properties of their respective owners. Features and specifications are subject to change without notice.