

ServSec HSM User Manual

V1.0

Contents

1	Introduction	1
	Module Overview.....	1
	Service Functions	1
	Block Diagram	2
2	Module Installation	3
	Module Operating Connections.....	3
	Module Start Up.....	3
3	HSM Touch Screen Functions.....	4
	3.1 Module Initialization.....	4
	3.1.1 Initialization Process	4
	3.1.1.2 Operation Procedure	4
	3.1.2 Re-Initialization	10
	3.1.2.2 Operation Procedure	10
	3.2 Authentication to Boot	13
	3.3 Remake Authentication card.....	16
	3.4 Authentication Card PIN Modification.....	19
	3.5 Start/Stop Service.....	20
	3.6 Setting up.....	23
	3.7 Device Info	26
4	HSM management.....	28
	4.1 Installation Management tool.....	28
	4.2 Management tool connection.....	32
	4.3 Logon/logout.....	32
	4.4 Manager Roles and Access Rights	33
	4.4.1 System Manager	34
	4.4.1.1 Operator management	34
	4.4.1.2 White list management.....	39
	4.4.1.3 View device information	42
	4.4.2 Safe Manager.....	43
	4.4.2.1 Symmetric key management	44
	4.4.2.2 Asymmetric key management	50
	4.4.2.3 View device information	55
	4.4.3 Audit Manager	56
	4.4.3.1 Logs	57
	4.4.3.2 Operator log.....	59
	4.4.3.3 Configuring Running Log Parameters.....	61
	4.4.3.4 Check the running log	62
	4.4.3.5 Check device network configuration	63
	4.4.3.6 View Device Information.....	64
5	Application System Connection	66
	5.1 API Model.....	66
	5.2 Integration Process.....	66
6	Note	68

1 Introduction

Module Overview

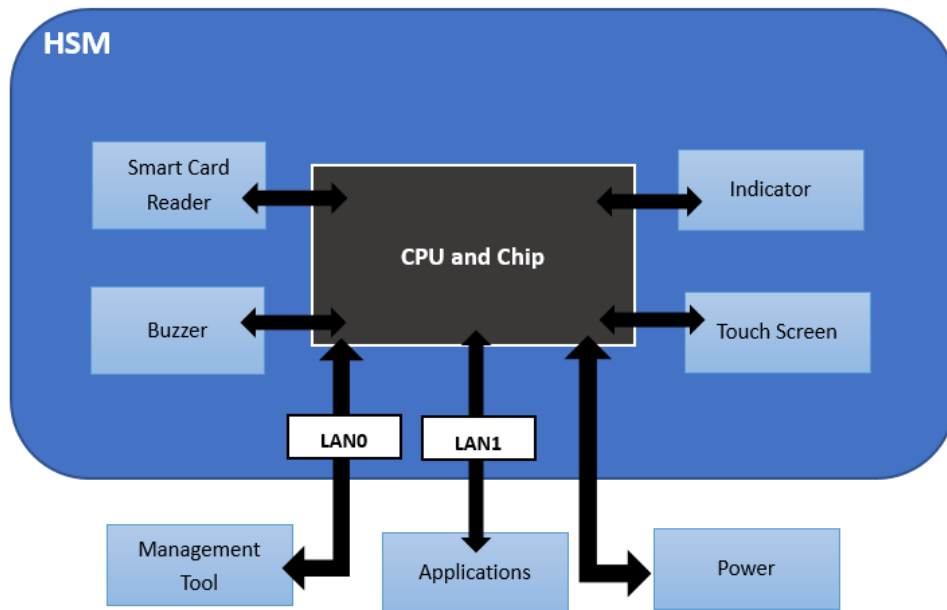
HSM is a high-performance crypto service module. It provides crypto services and management through an Ethernet port, and supports touch screen operations and card readers for smart card-based ID verification and authorization.

Service Functions

HSM mainly supports the following crypto services:

- 1) encrypted storage and transmissions for sensitive data
- 2) message integrity verification
- 3) asymmetric/symmetric algorithms
- 4) security management functions such as key generation, distribution, transportation, storage, and key management
- 5) smart card with secure functionalities adopted as operation management access control media for authentication
- 6) providing multi secure services such as asymmetric signature/verification, hash digest generation, symmetric data encryption/decryption.

Block Diagram



2 Module Installation

Module Operating Connections

HSM is installed inside the local network as a crypto server, where LAN1 is HSM service port and the local host/application server is connected to HSM via local network to use the services provided by HSM. LAN0 is the HSM configuration port. The management client is connected to HSM via this port to implement configuration management on HSM.

Module Start Up

After powering on, HSM will start. The switch button is located on the front of the HSM case. When the button is pushed, the red LED (power indicator) will light up. HSM will start its self-test. If the self-test fails, the touch screen will show the reason for the failure and a yellow LED (error indicator) will light up along with an alarm sound; if self test succeeds, the touch screen will show the initialization page and the blue LED (waiting for initialization status indicator) will light up.

Click initialization and follow the instructions to implement initialization for Device Manager (Dev-Manager), System Manager (Sys-Manager), Safe Manager (Safe-Manager), and AuditManager (Audit-Manager). Once initialization is complete, the module will enter start service selection program. Before starting services, a System Manager card authentication will be required. After service starts, the green LED (working status indicator) will light up and the device will enter normal working status.

Note: Once HSM has started successfully, the red LED (power indicator) will remain lit.

3 HSM Touch Screen Functions

3.1 Module Initialization

Module initialization operation is performed using the touch screen. Module initialization mainly contains operations for Device Manager authentication card generation, component key generation, component key protection password configuration, System Manager/Manager/Safe Manager/Audit Manager authentication card generation, etc. Once initialization is successful, the module will enter Device Manager authentication start up page. Module initialization is divided into original initialization and re-initialization. Once the self test is passed, the module will detect if initialization is done automatically. If yes, the module will enter page **【Auth2Boot】** & **【InitAgain】** ; if no, the module will enter page **【Init】** .

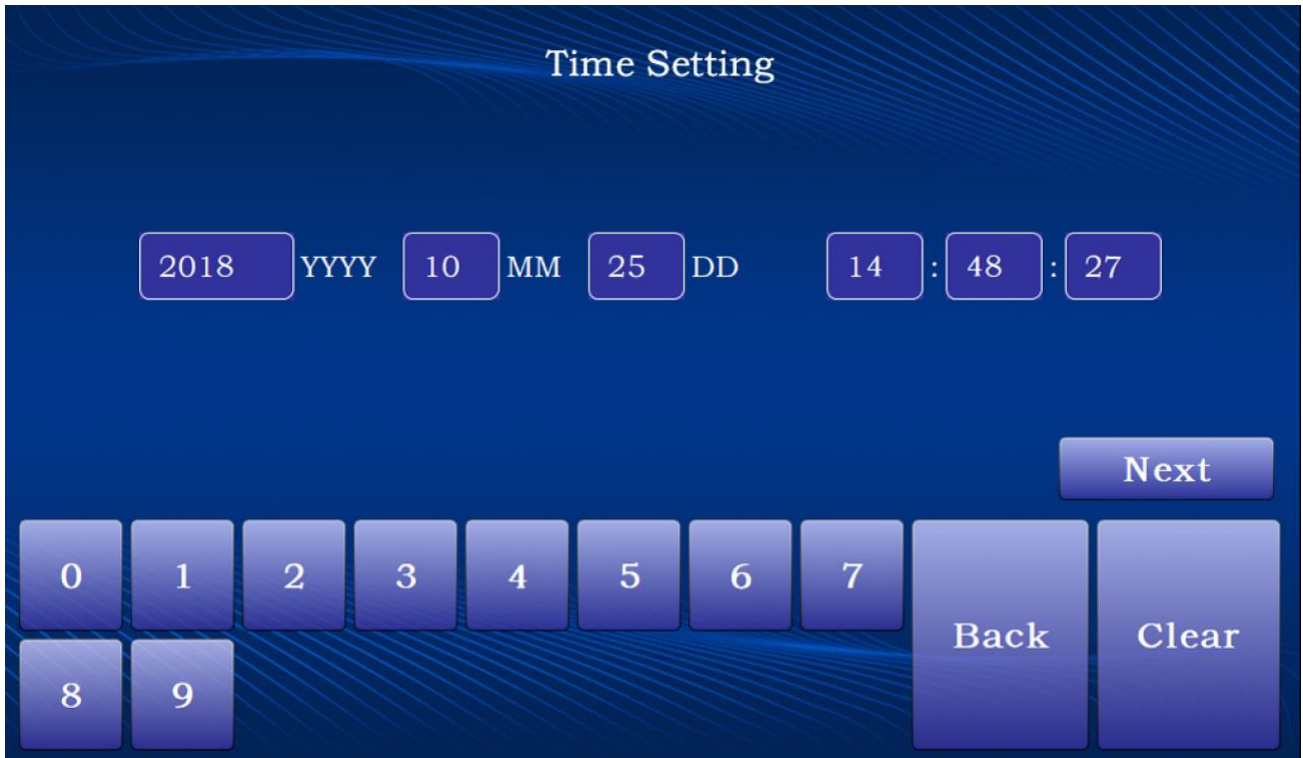
Note:1. Before initialization, we highly recommend marking the authentication card to be initialized; which are divided into Device Manager A1 card, Device Manager A2 card, Device Manager A3 card, System Manager B card, Safe Manager C card and Audit Manager D card, so the operator can avoid confusion on different cards in initializing authentication cards.

2. When inserting an authentication card, keep the card chip facing down.

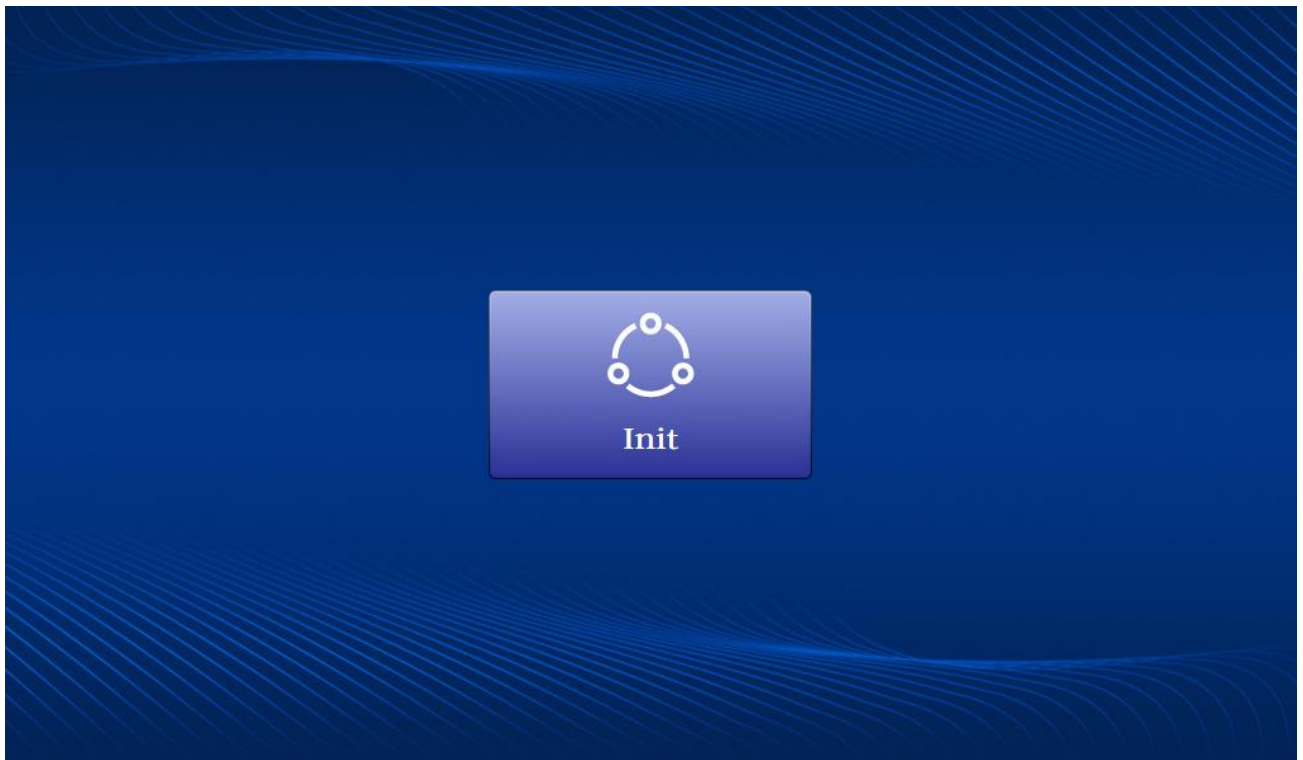
3.1.1 Initialization Process

3.1.1.2 Operation Procedure

Device first switches on. After passing the self-test, the touch screen will display the Time Setting screen by default.



After setting time, click **【Next】** to continue the initialization process.



Initialize device manager

Click **【Init】** and start the manager initialization according to touch screen instructions. Insert the Device Manager authentication card and set the 8-digit authentication card password.

Init Dev-Manager(A1) - Set Card-PIN

Card-PIN 00

Confirm Card-PIN 00

▲ Please insert a new card(A1), and set PIN(8 chars must contain No. & char).

0	1	2	3	4	5	6	7	Back	Clear
8	9	A	B	C	D	E	F		

Click **【Next】** , then set the 32 digit MK component and 8 digit component protection password.

Init Dev-Manager(A1) - Set MK-Part

MK-Part 00

Confirm MK-Part 00

MK-Part-PIN 00

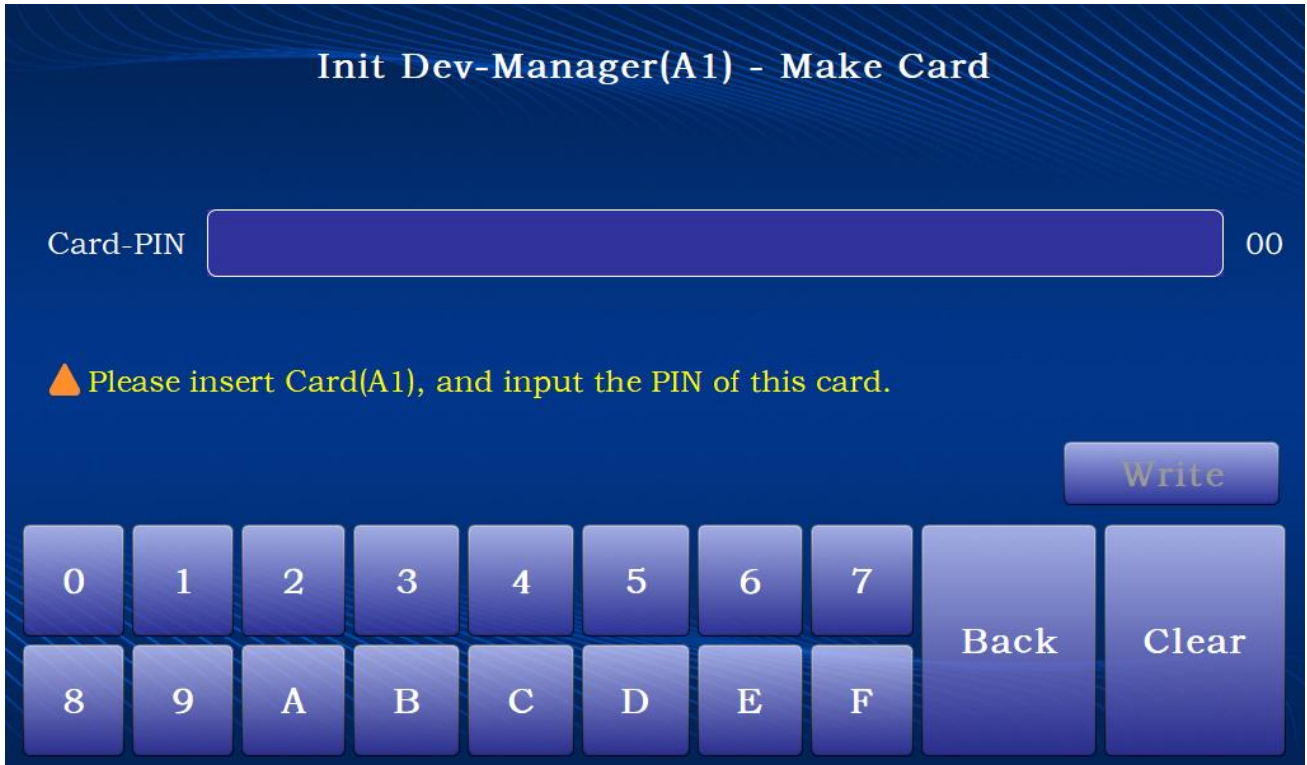
Confirm MK-Part-PIN 00

0	1	2	3	4	5	6	7	Back	Clear
8	9	A	B	C	D	E	F		

Repeat the procedures above. Initialize in turn each Device Manager A1, A2, A3 cards and set MK component and component key protection password.

After the 3 Device Managers are set, insert each of the 3 Device Manager authentication cards one after

another. Input configured authentication card password to verify. Click **【Write】**, then perform the card writing process, as shown in the figure below:



After initializing the Device Manager, the operator can perform initialization processes on other managers, as shown in the figure below:



Initialize System Manager:

Click **【Sys-Manager】** and insert an authentication card according to touch screen instructions. Set working key and authentication card password, and perform the card making process.

Init System-Manager(B1) - Set Card-PIN

Factor 00

Card-PIN 00

Confirm Card-PIN 00

▲ Please insert a new card(B1), and set PIN(8 chars must contain No. & char).

Cancel Make

0 1 2 3 4 5 6 7 Back Clear

8 9 A B C D E F Back Clear

Note: System Manager cannot be generated afterwards. User can make multiple System Manager authentication cards as a backup.

Initialize Safe Manager:

Click **【Safe-Manager】** and insert an authentication card according to touch screen instruction. Set authentication card password and perform the card making process.

Init Safe-Manager(C1) - Set Card-PIN

Card-PIN 00

Confirm Card-PIN 00

▲ Please insert a new card(C1), and set PIN(8 chars must contain No. & char).

Cancel Make

0	1	2	3	4	5	6	7	Back	Clear
8	9	A	B	C	D	E	F		

Initialize Audit Manager:

Click **【Audit-Manager】** and insert an authentication card according to touch screen instructions, set authentication card password, and perform the card making process.

Init Audit-Manager(D1) - Set Card-PIN

Card-PIN 00

Confirm Card-PIN 00

▲ Please insert a new card(D1), and set PIN(8 chars must contain No. & char).

Cancel Make

0	1	2	3	4	5	6	7	Back	Clear
8	9	A	B	C	D	E	F		

Once initialization of all managers is finish and HSM initialization is finished, click **【Restart】** to restart HSM.

■ All Cards've already finished, please restart.



3.1.2 Re-Initialization

3.1.2.2 Operation Procedure

When the module has restarted, you can choose to reinitialize.



When the module is reinitialized, all current data stored in the module will be cleared. Once the operation is

finished, the data cannot be restored.

Re-initialization requires verification on any 2 of the 3 device managers. The authentication card should be inserted for verification. Input authentication card password and component key protection password to perform ID verification, as shown in the figure below:

ReInit - Auth any Dev-Manager

Card-PIN 00

MK-Part-PIN 00

▲ Please insert Card: any Dev-Manager

Cancel Next

0	1	2	3	4	5	6	7	Back	Clear
8	9	A	B	C	D	E	F		

ReInit - Auth another Dev-Manager

Card-PIN 00

MK-Part-PIN 00

▲ Please insert Card: another Dev-Manager

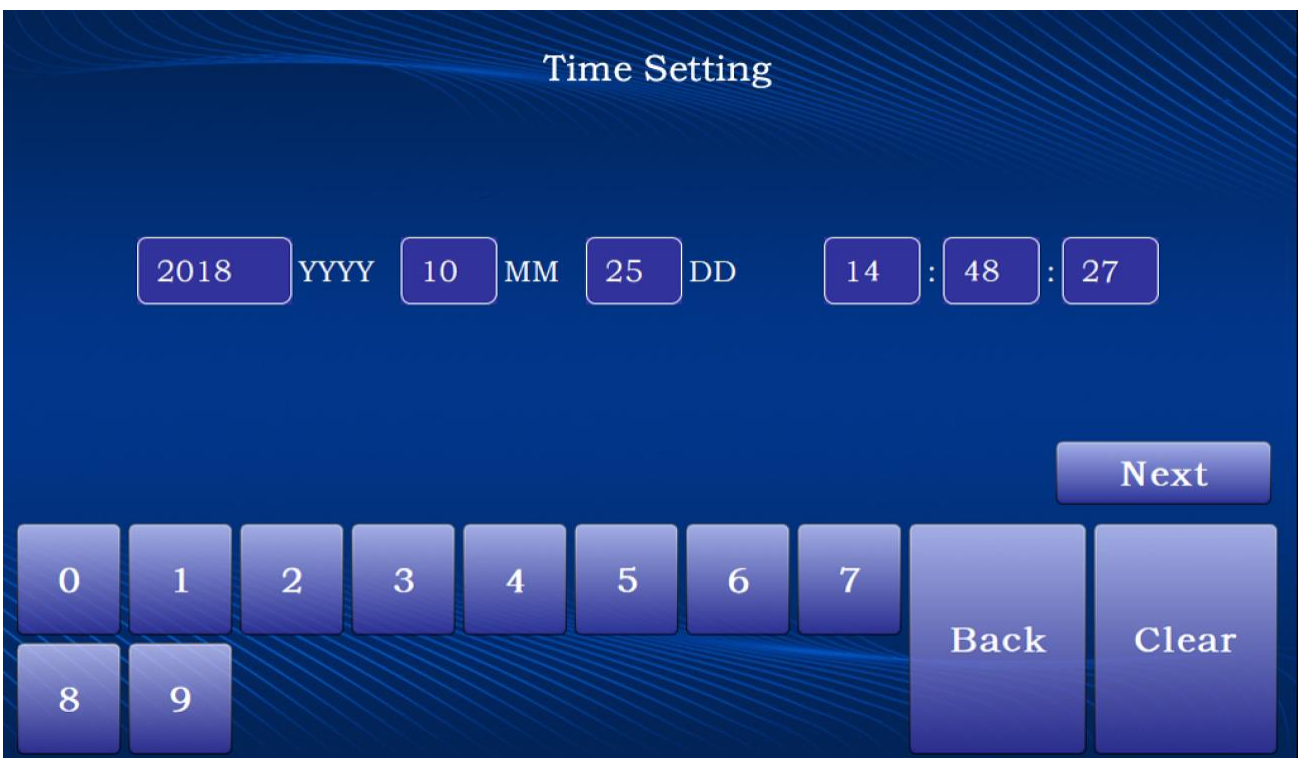
Cancel Next

0	1	2	3	4	5	6	7	Back	Clear
8	9	A	B	C	D	E	F		

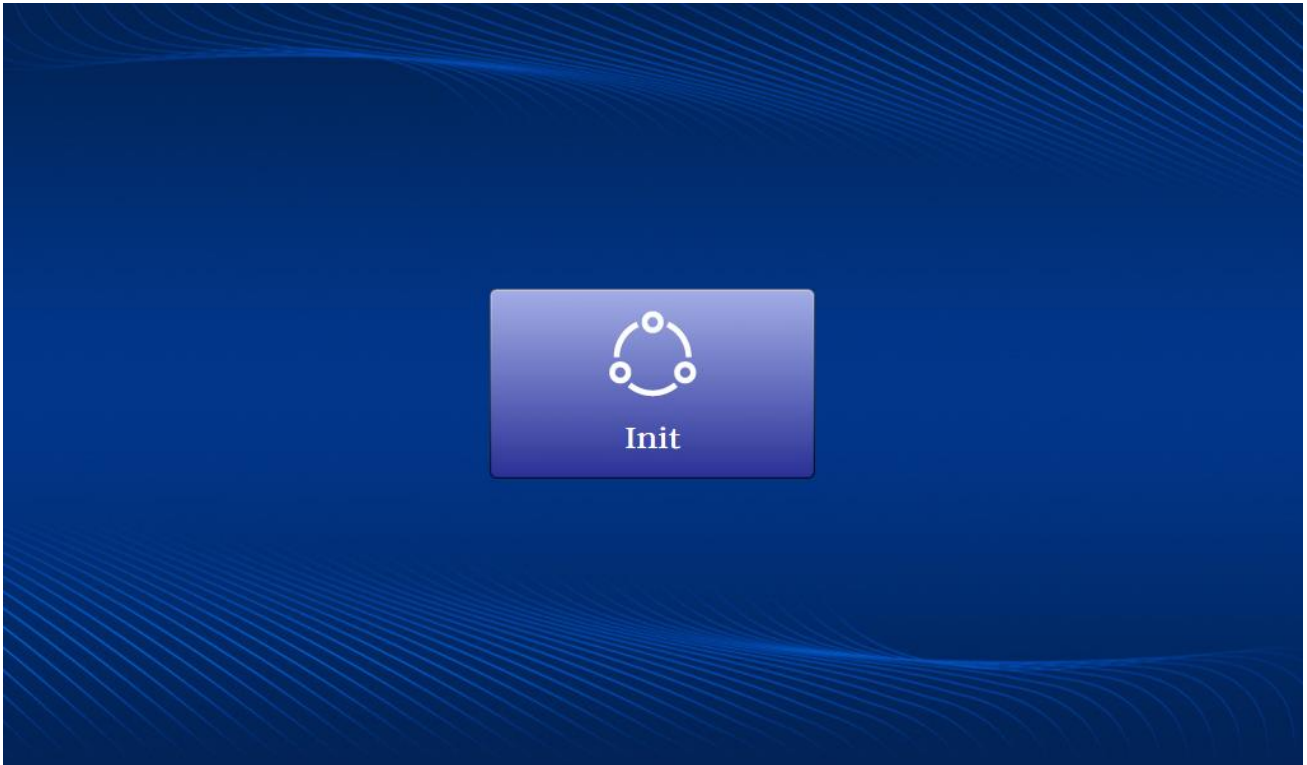
Once Authentication passed, click **【InitAgain】** , start re-initialization, as shown in the figure below:



After starting reinitialization, you will enter the Time Setting screen:



Once you've finished making your settings selection, click **【Init】** to start initialization.



For detailed initialization process, please refer to section 3.1.1.

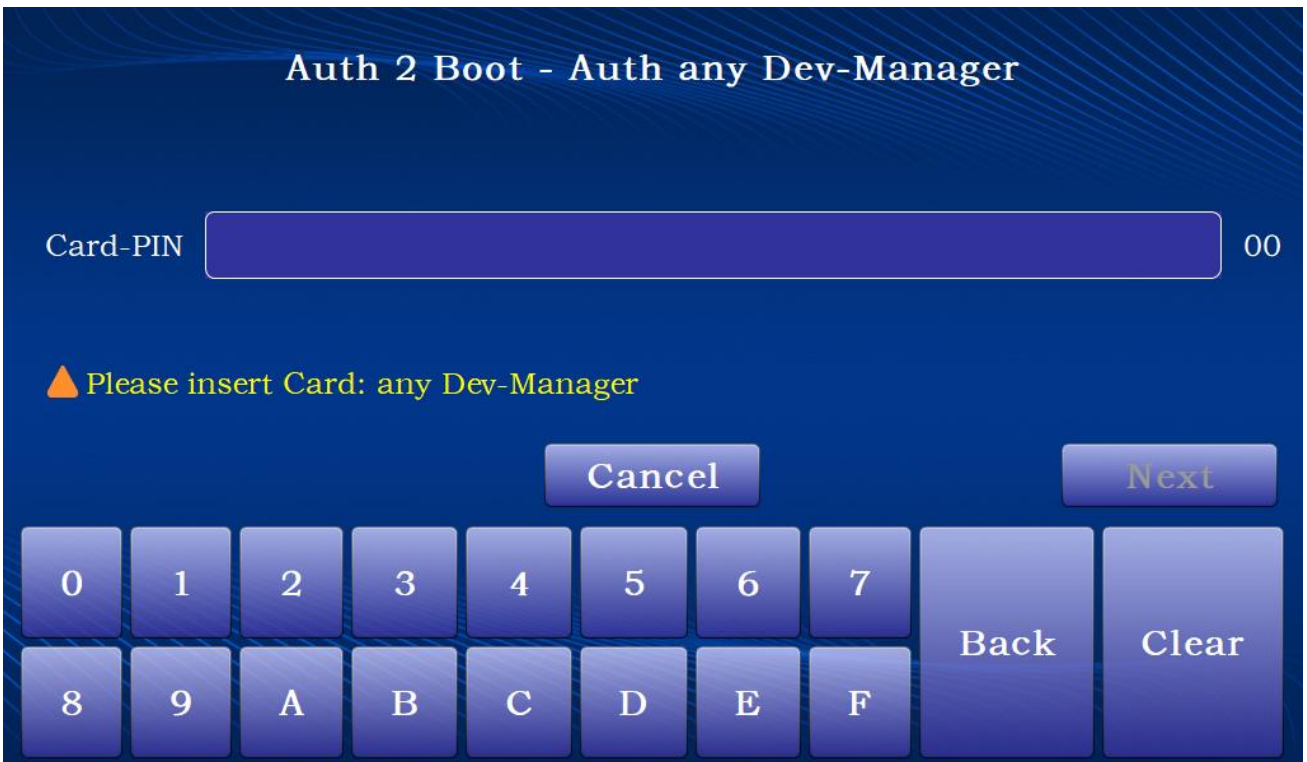
3.2 Authentication to Boot

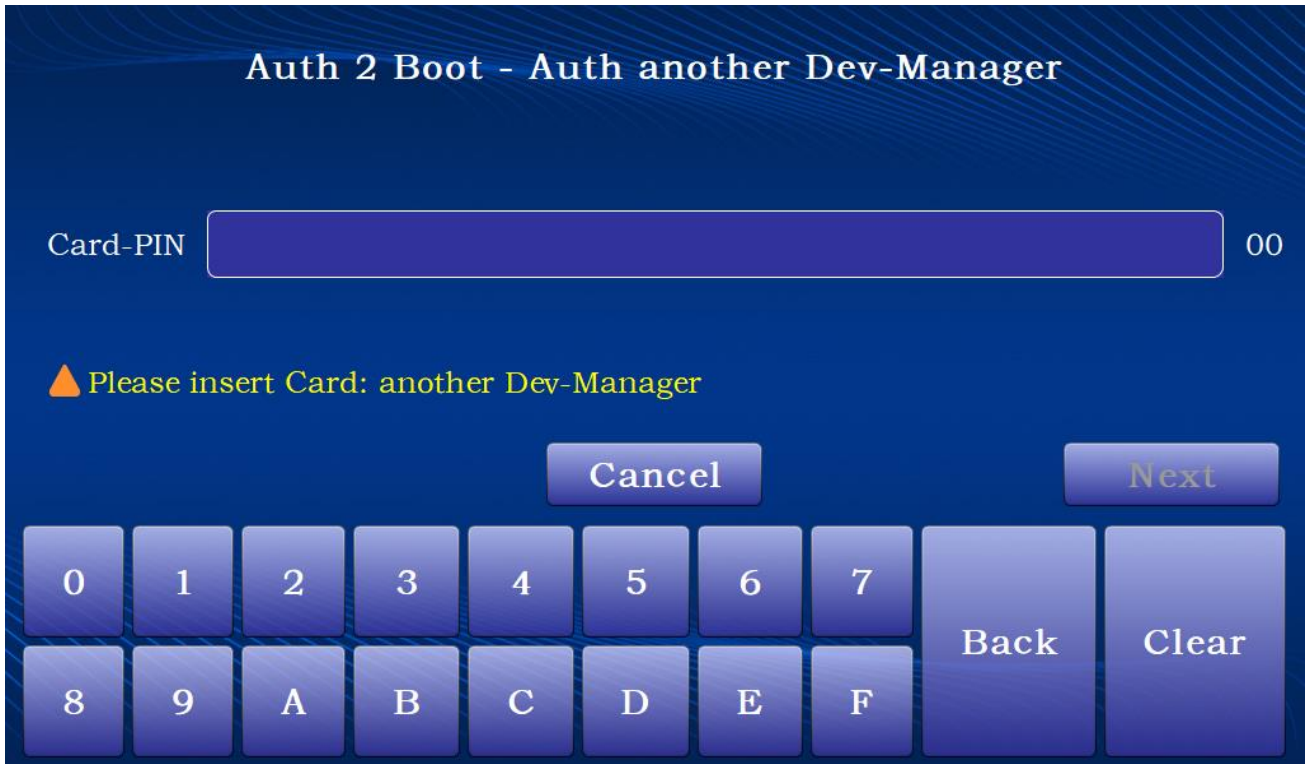
When HSM is initialized, push the switch on/off button on the HSM. The touch screen will load the start screen.



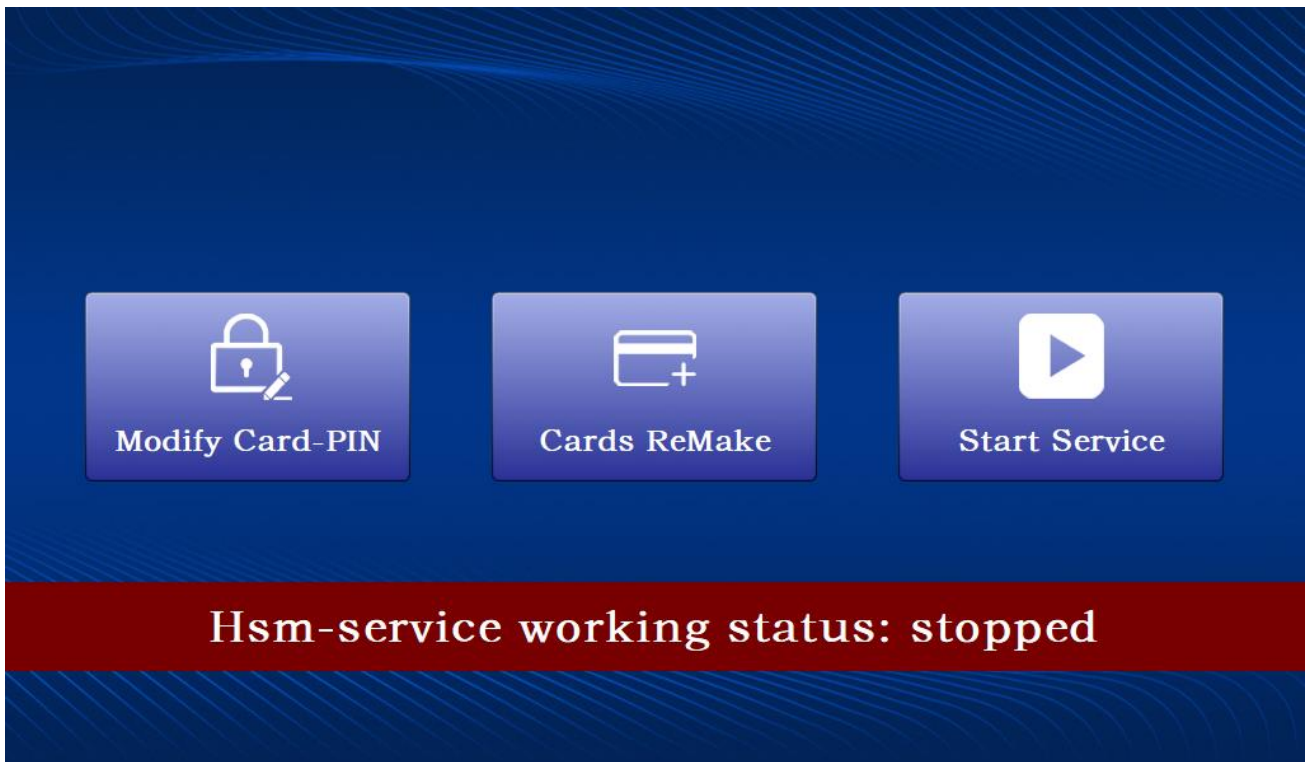
To switch on the HSM, it requires 2 of 3 Device Managers to perform ID verification to authenticate.

Click **【Auth2Boot】**, enter Device Manager authentication screen, insert Device Manager authentication card and input password to perform ID verification.





Verify 2 Device Managers. Once verified, the authentication card password is changed and the authentication card regenerates. Service start will be allowed and crypto service status will be displayed at bottom of touch screen.



3.3 Remake Authentication card

If the Device Manager or the authentication card is lost, the operator can remake the authentication card.

Note: System Manager authentication card cannot be remade.

After authentication is switched on, click **【Cards ReMake】**, enter Cards ReMake page. You can choose to remake the authentication cards for the roles of Device Manger, Safe Manager, and Audit Manager.



Remake Device Manager card

Click **【Device-Manager】**, input the MK-Part-PIN (the component key protection password) for the Device Manager authentication card to be remade:

ReMake Dev-Manager(A)

MK-Part-PIN 00

▲ Please input the MK-Part-PIN of the card you will re-init.

Cancel Next

0	1	2	3	4	5	6	7	Back	Clear
8	9	A	B	C	D	E	F		

Once verification is completed, click **【Next】** to enter the ReMake Dev-Manager(A) screen. Insert a new authentication card and set the card PIN.

ReMake Dev-Manager(A)

Card-PIN 00

Confirm Card-PIN 00

▲ Please insert a new card(A), and set PIN(8 chars must contain No. & char).

Cancel OK

0	1	2	3	4	5	6	7	Back	Clear
8	9	A	B	C	D	E	F		

Click **【OK】** to make the authentication card. Once completed, the new authentication card will replace the previous authentication card.

Note: After the authentication card is remade, the Device Manager can only use the new card for ID verification.

Remake Safe Manager card

Click **【Safe-Manager】**, then insert a new card and input the card PIN. Click **【OK】**.

ReMake Safe-Manager(C)

Card-PIN

Confirm Card-PIN

▲ Please insert a new card(C), and set PIN(8 chars must contain No. & char).

Cancel OK

0	1	2	3	4	5	6	7	Back	Clear
8	9	A	B	C	D	E	F		

Remake Audit Manager card

Process is identical to remaking Safe Manager card.

ReMake Audit-Manager(D)

Card-PIN

Confirm Card-PIN

▲ Please insert a new card(D), and set PIN(8 chars must contain No. & char).

Cancel OK

0	1	2	3	4	5	6	7	Back	Clear
8	9	A	B	C	D	E	F		

3.4 Authentication Card PIN Modification

This function is used to modify a manager's authentication card PIN.

After turning on HSM, click **【Modify Card-PIN】**, enter the authentication card PIN modification screen, and insert the card associated with the PIN to be modified. Input the old PIN, then enter the new PIN and confirm the PIN. Click **【OK】**. Once the PIN has been successfully modified, the manager can only use new the new PIN to verify their ID.

Modify Card-PIN

Old Card-PIN 00

New Card-PIN 00

Confirm New Card-PIN 00

▲ Please insert Card, and set PIN(8 chars must contain No. & char).

Cancel OK

0	1	2	3	4	5	6	7	Back	Clear
8	9	A	B	C	D	E	F		

3.5 Start/Stop Service

Start/stop service requires System Manager verification and authentication before completing the operation.

Start service:

After turning on the HSM, click **【Start Service】**, insert System Manager authentication card, and enter card PIN.

Start Service - Authentication

Card-PIN

▲ Please insert System-Manager Card, and input the PIN of this card.

Cancel Next

0	1	2	3	4	5	6	7	Back	Clear
8	9	A	B	C	D	E	F		

Once the System Manager is successfully verified, enter the configurations for the following items:

- Managed-Netcard(M-Net0) IP (management network adaptor IP) and its associated port
- Applied-Network(A-Net1) IP (application network adaptor IP) and its associated port

Click **【Start】** when done.

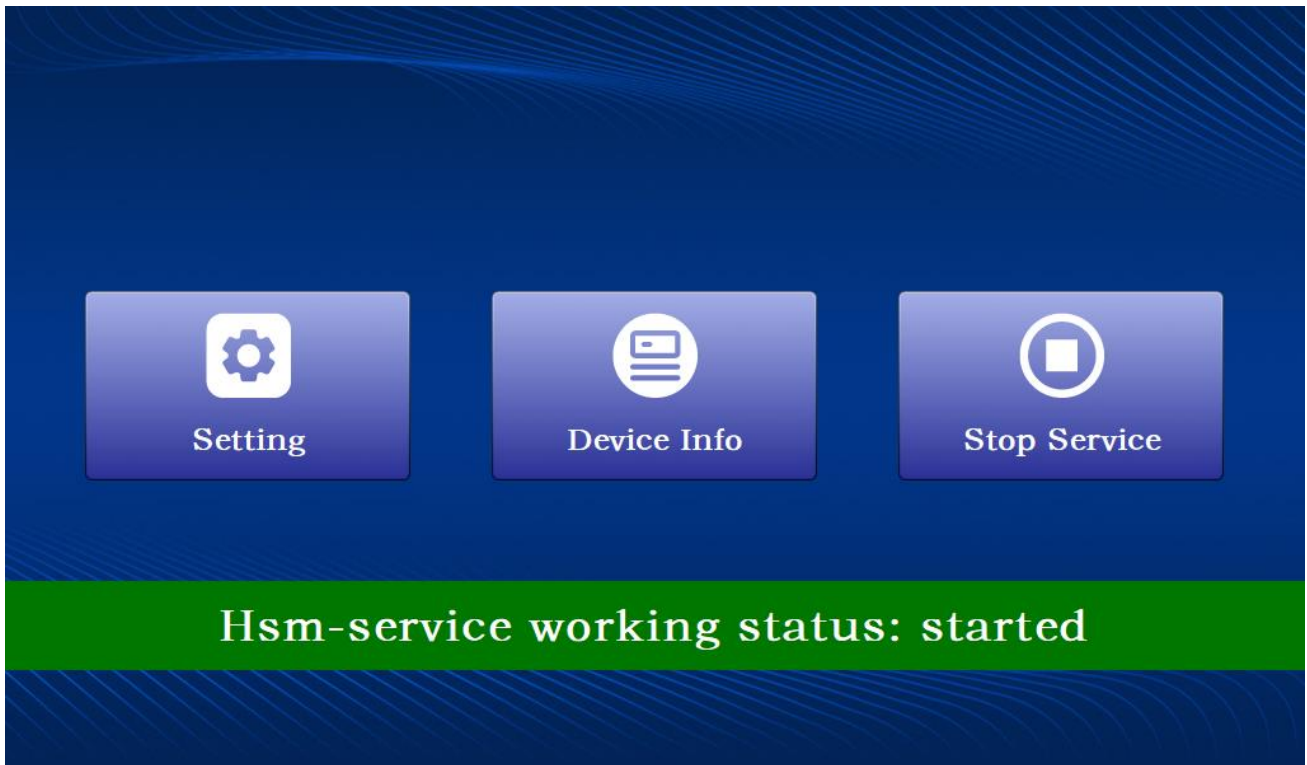
Start Service - Setting

	IP address	Port	Subnet mask	Default gateway
M-Net0:	<input style="width: 150px;" type="text" value="192.168.25.224"/>	<input style="width: 60px;" type="text" value="1812"/>	<input style="width: 150px;" type="text" value="255.255.255.0"/>	
A-Net1:	<input style="width: 150px;" type="text" value="192.168.25.225"/>	<input style="width: 60px;" type="text" value="1813"/>	<input style="width: 150px;" type="text" value="255.255.255.0"/>	<input style="width: 150px;" type="text" value="192.168.25.254"/>

Cancel Start

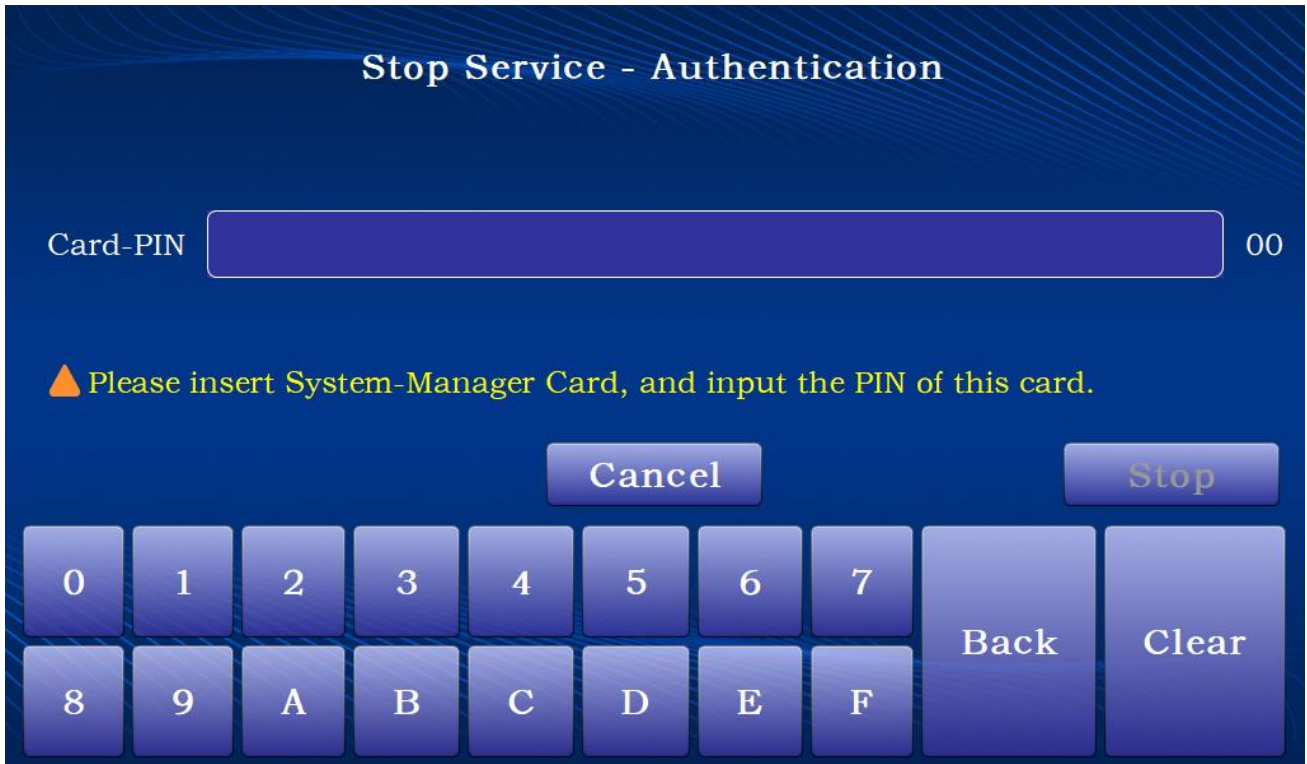
0	1	2	3	4	5	6	7	Back	Clear
8	9	.							

Once service has started, the options to stop service, change settings, and review device information will be allowed. The status of the HSM will be displayed at the bottom of the touch screen.



Stop service:

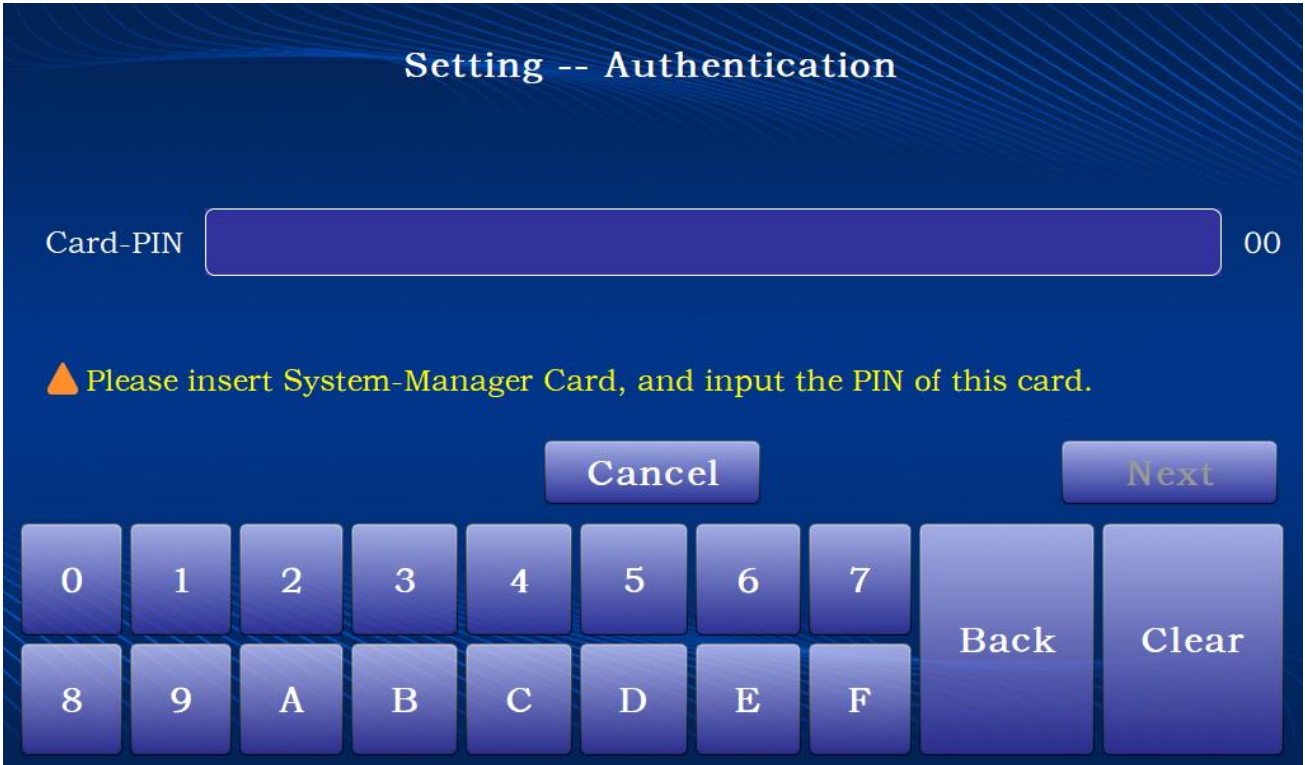
After starting service, click **【Stop Service】**, insert System Manager authentication card, and input card PIN for verification. If verified, service will stop.



3.6 Setting up

This module can set up and manage IP whitelist in client side, and set the system time.

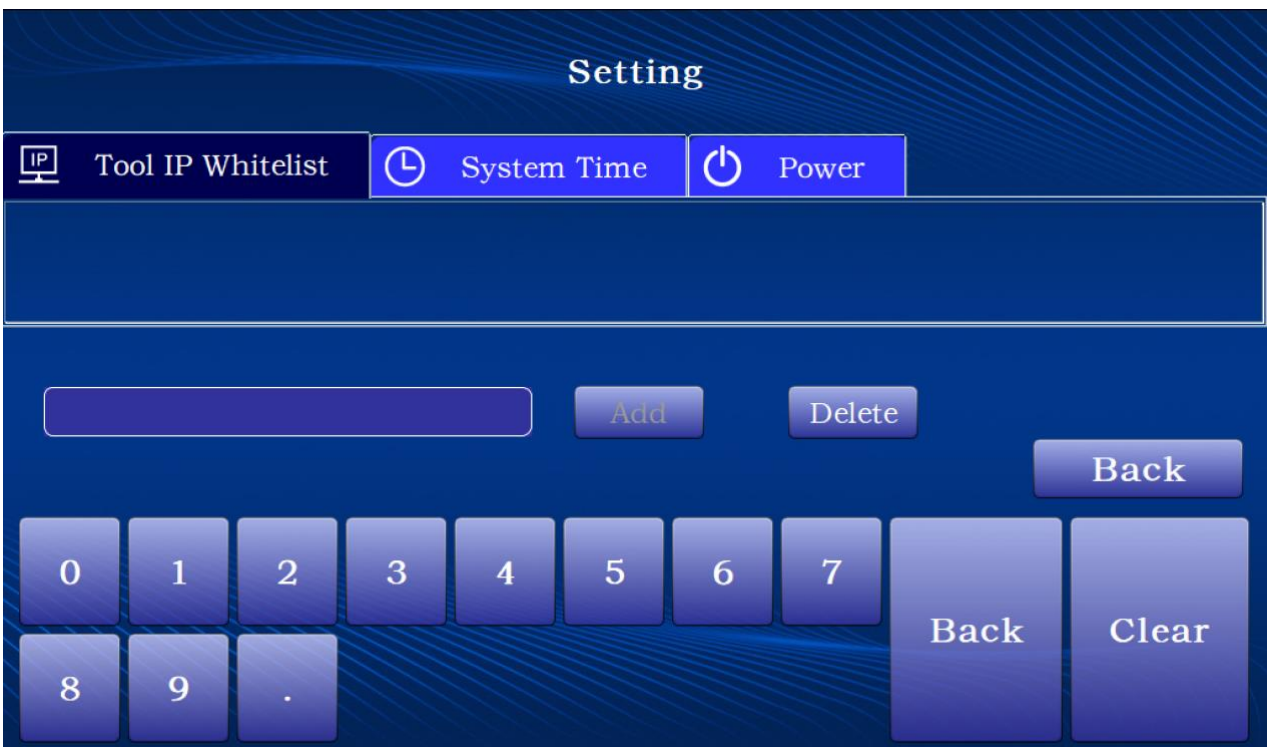
After starting service, click **【Setting】**, insert System Manager authentication card, then input card PIN for verification to enter the Setting -- Authentication screen.



Set/manage IP white list in client side

With the client OP white list, the management tool on a client connected to the HSM is allowed to connect to the module to add, delete, and review these IPs.

Click **【Tool IP White list】**, switch to management tool IP white list setting page, can review all allowed IPs, as shown in the figure below:

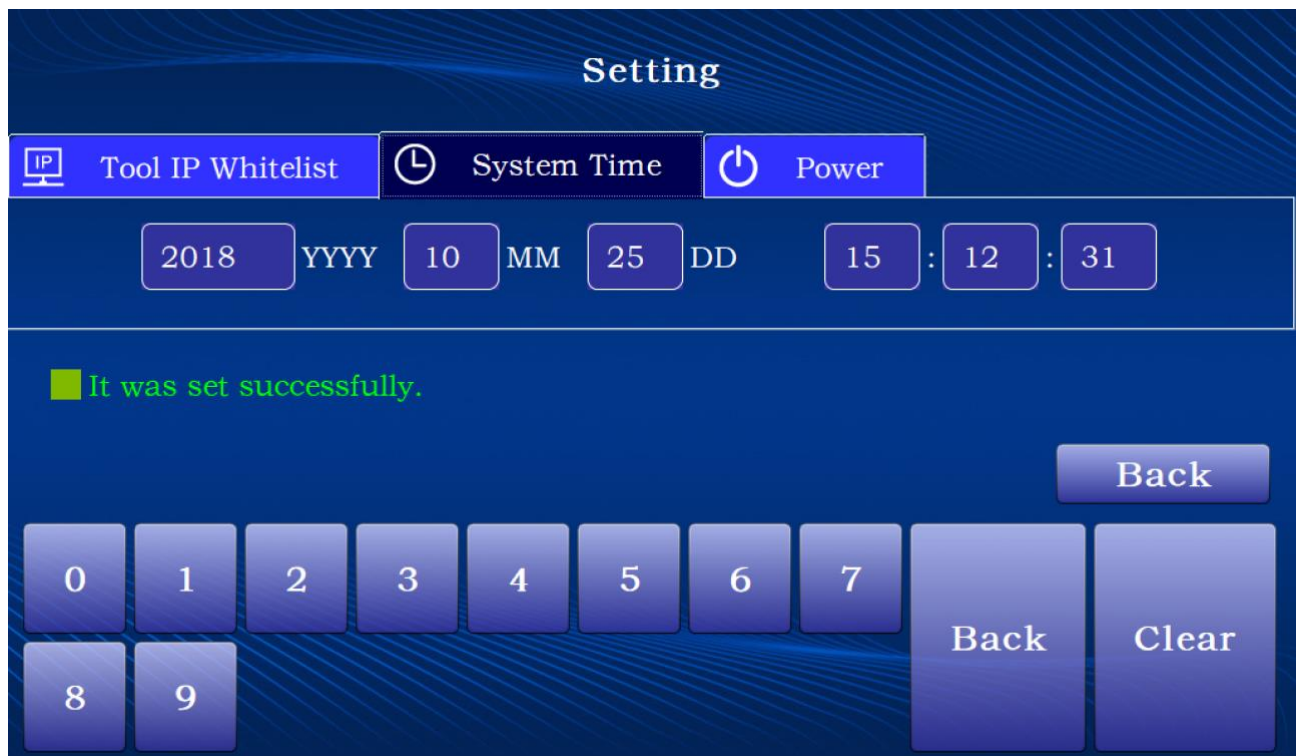


Add: Input IP address to be added and click **【add】**. When successful, it will allow this IP address management tool client to visit.

Delete: Select one or more IP addresses and click **【delete】**. When deletion is successful, it will deny this IP address management tool client from visiting.

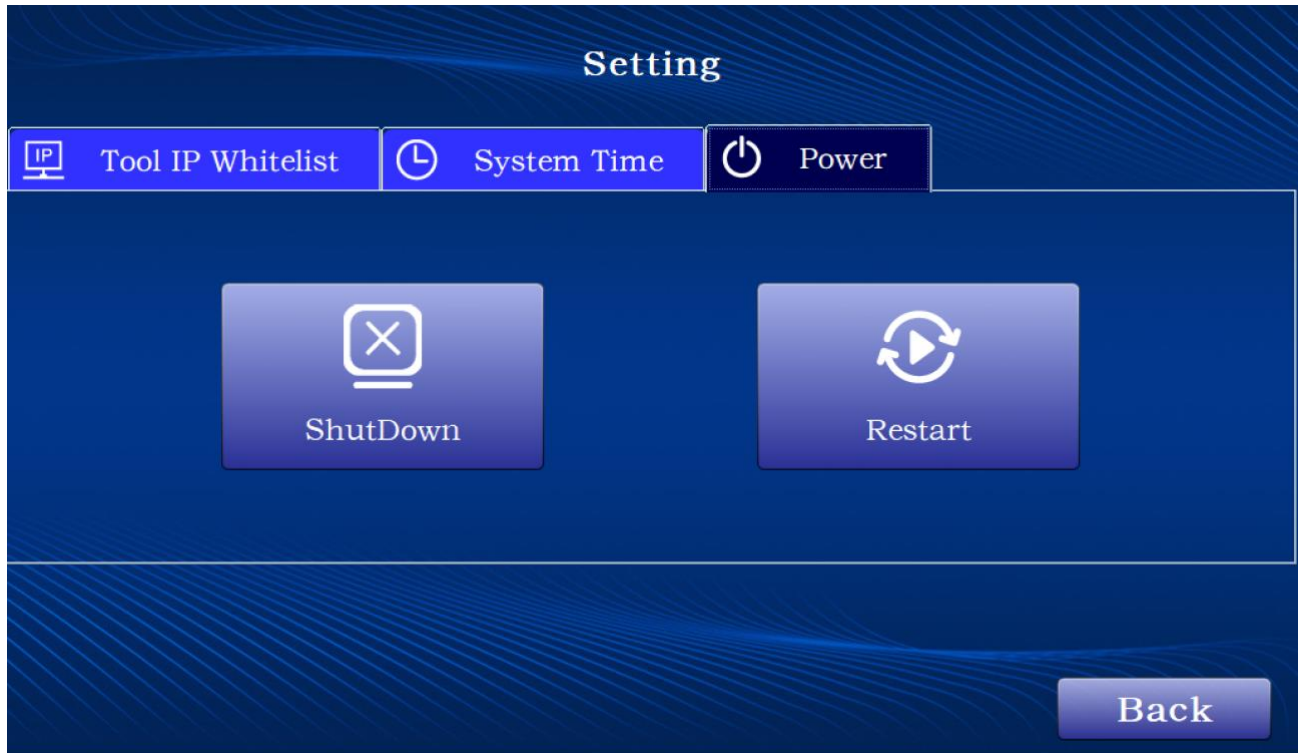
System time setting

Click **【System Time】**, switch to system time setting page, input correct date and time, setting finish, as shown in the figure below:



ShutDown& Restart

Click **【Power】**, switch to **【ShutDown& Restart】** page, and click **【ShutDown】** to shut down the module, or click **【Restart】** to restart the module as shown in the figure below:



3.7 Device Info

After service is started, the touch screen will display **【Stop Service】**、**【Setting】**、**【Device Info】** buttons. Click **【Device Info】** to view detailed device information, including the manufacturer:

Device Info

Manufacturer: FEITIAN Technologies Co., Ltd.
Device Name: FEITIAN ServSec HSM
Device Model Number: HSM V2.0
Software Version: 2.0.0
Device Key Check Value: 381081498babd47c67602723196f22235b635aed
1cb19c7284c33c65b5d257c2

M-Net0: Mac=00:00:00:00:00:00 Ip:port=192.168.25.224:1812
Mask=255.255.255.0 Gateway=192.168.25.254
A-Net1: Mac=00:00:00:00:00:00 Ip:port=192.168.25.225:1813
Mask=255.255.255.0 Gateway=192.168.25.254

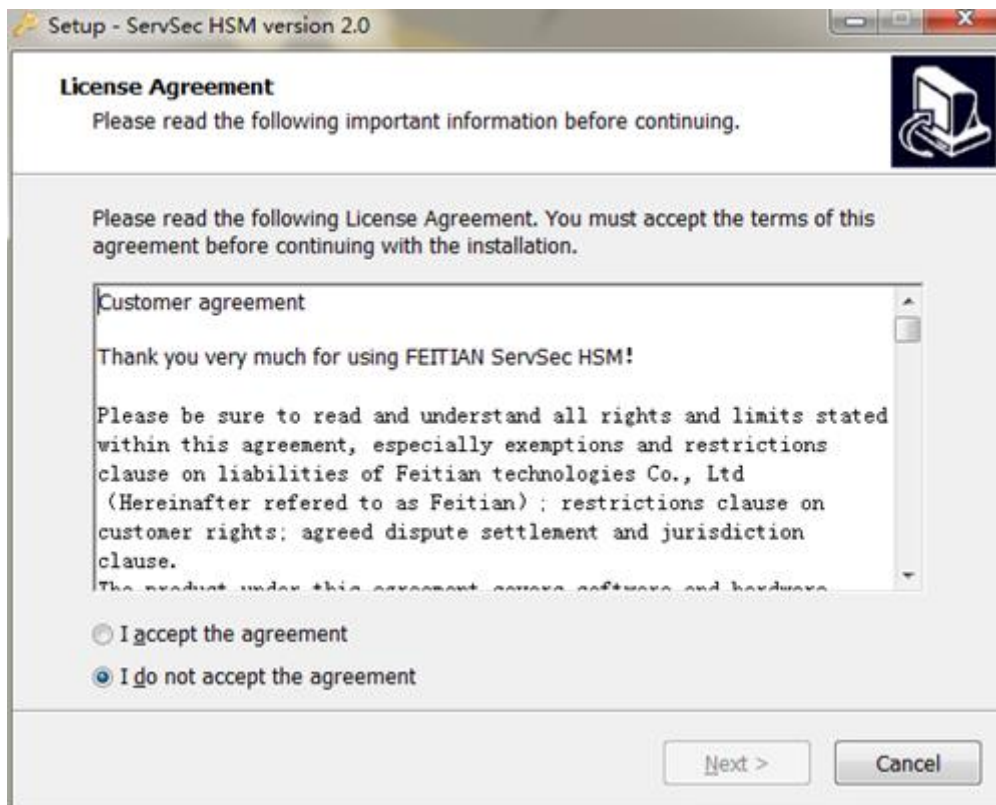
[Back](#)

4 HSM management

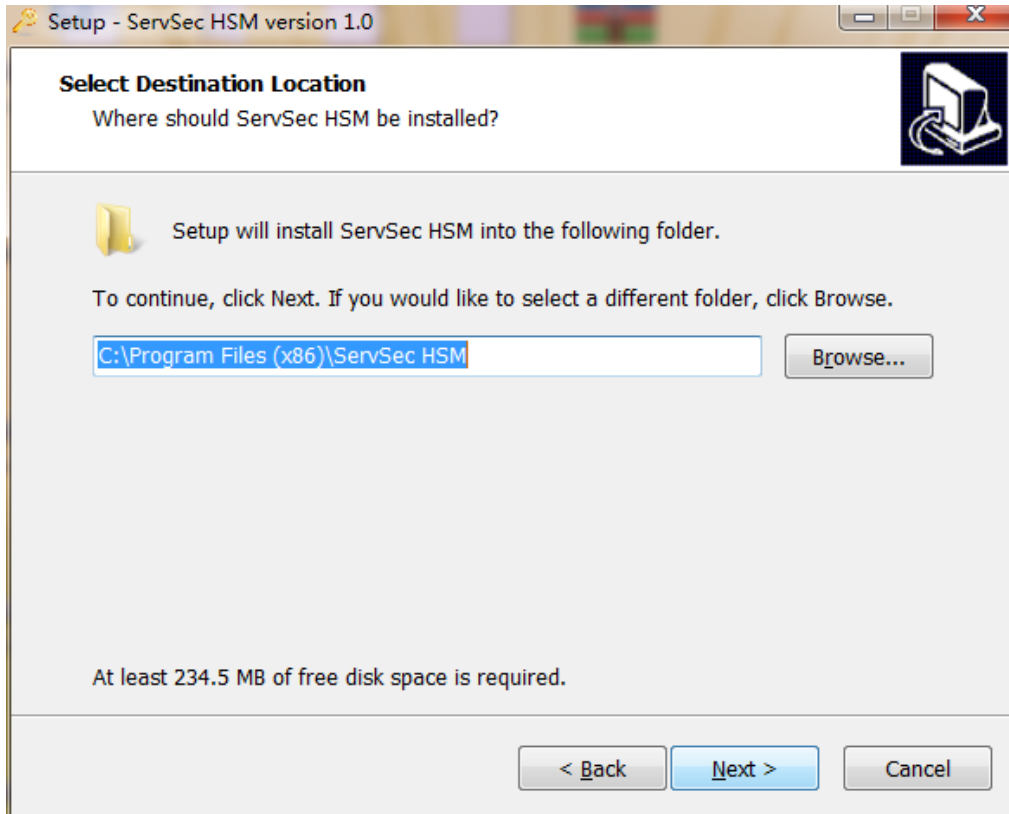
4.1 Installation Management tool

Operator can use the management tool to perform configuration management function on Windows PC. Management tool installation process is shown as below:

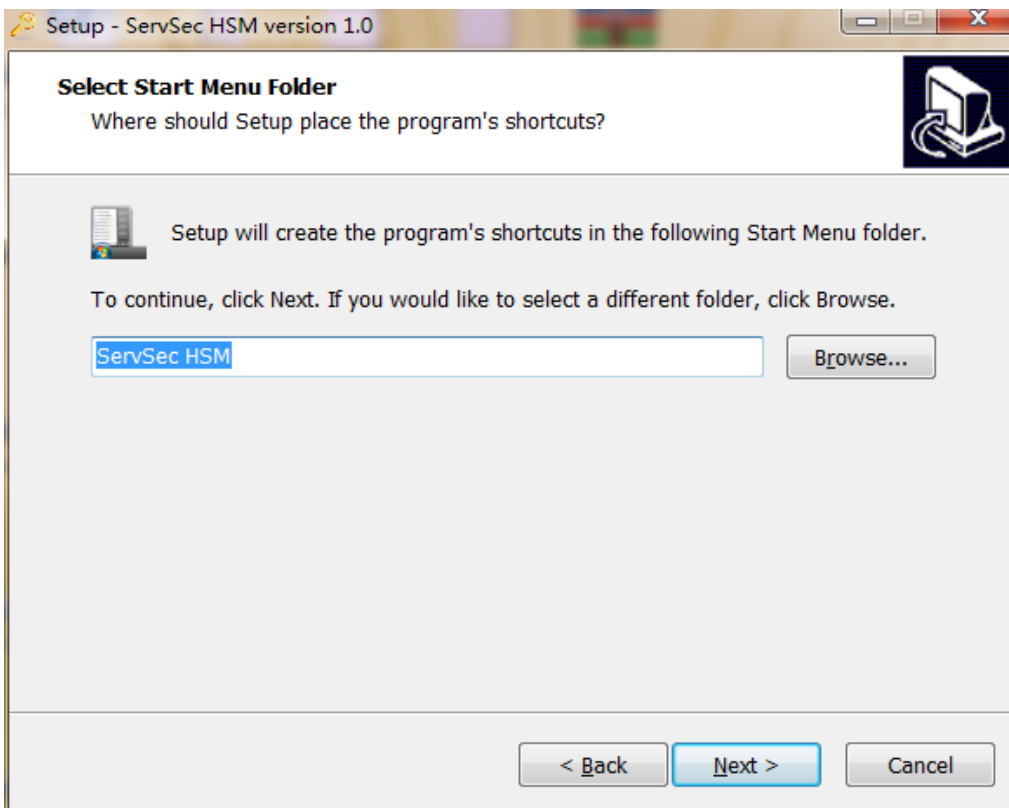
First executing “FthsmSetup.exe”, installation guide dialog box will popup, as shown below:



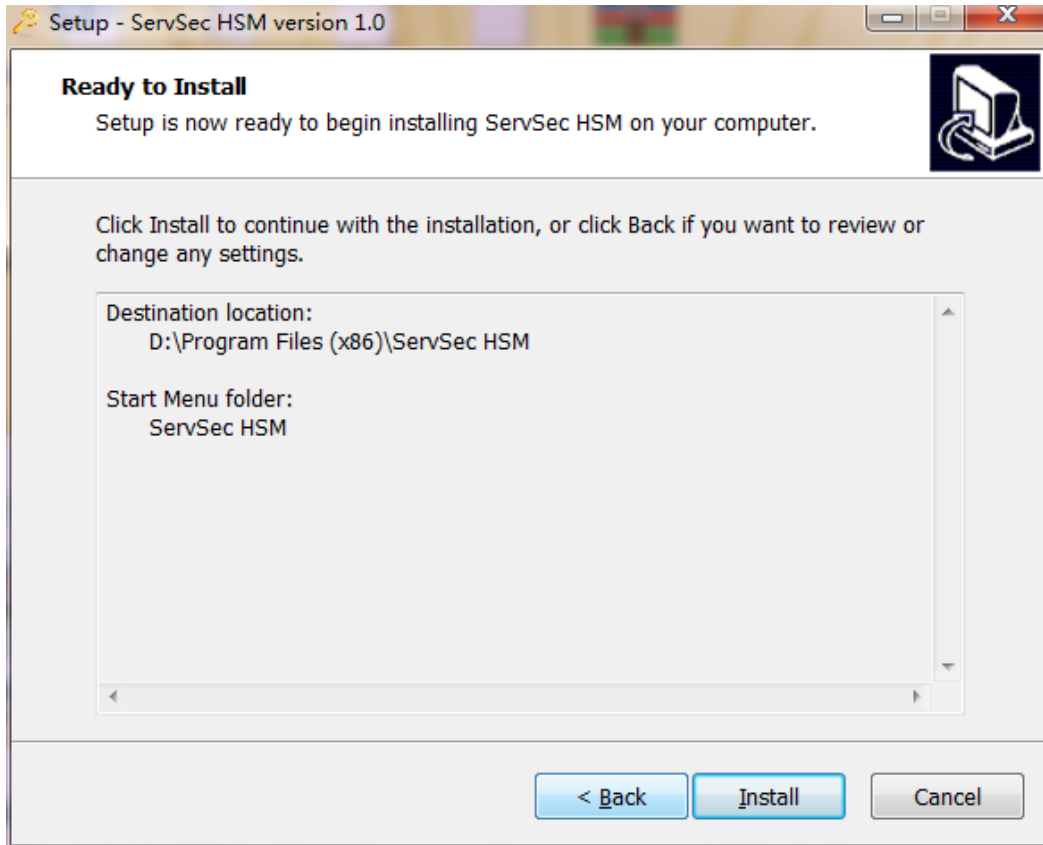
Click **【I accept the agreement】**, and click **【Next】**, installation directory selection dialog will popup, as shown below:



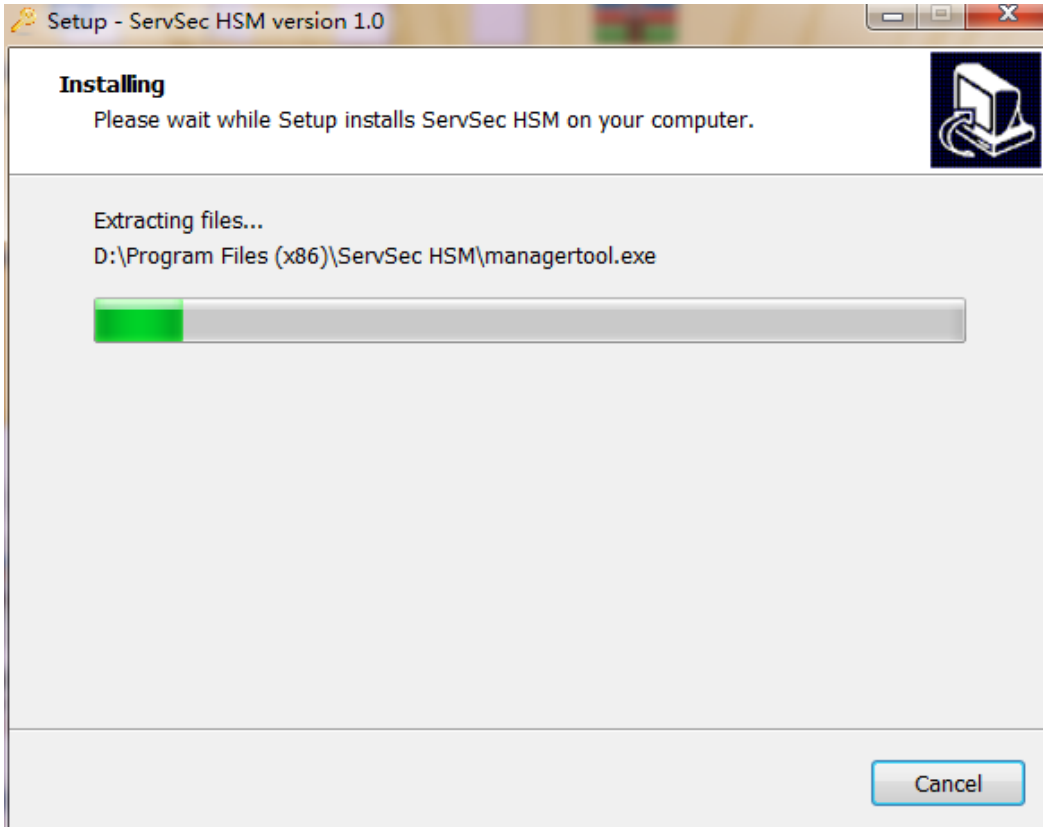
Click **【Next】**, shortcut placement dialog will popup:



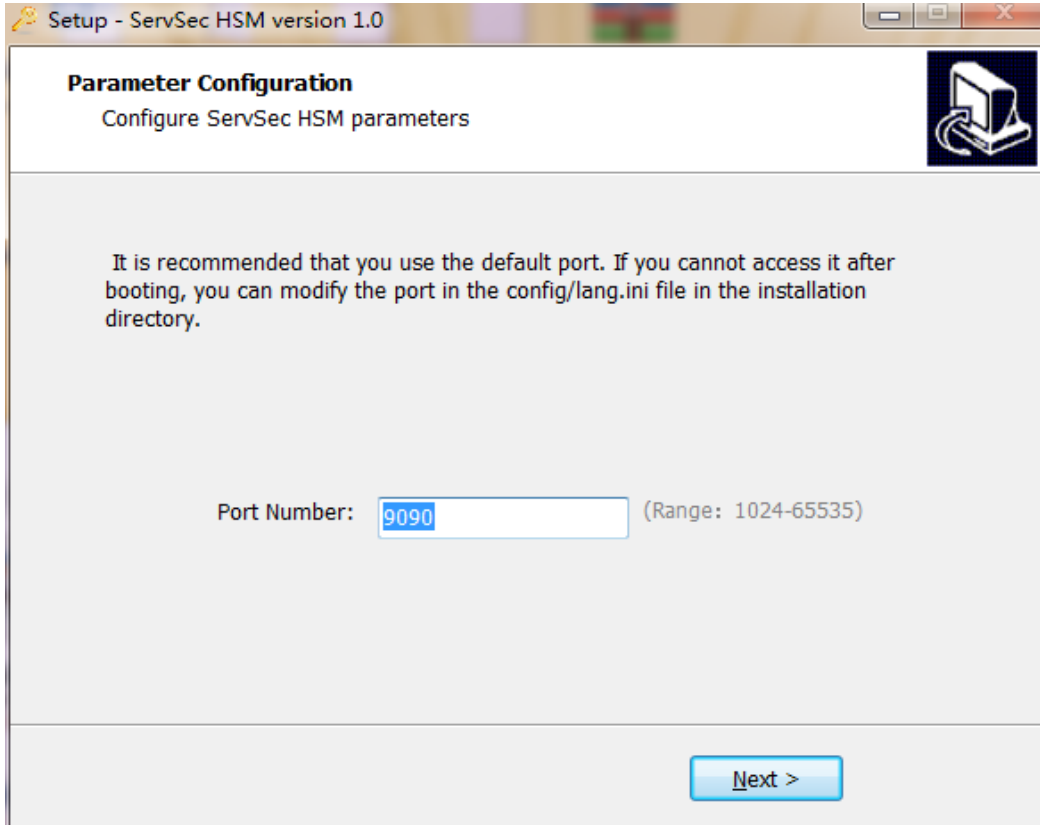
Click **【Next】**, installation preparation finished dialog will popup, as shown below:



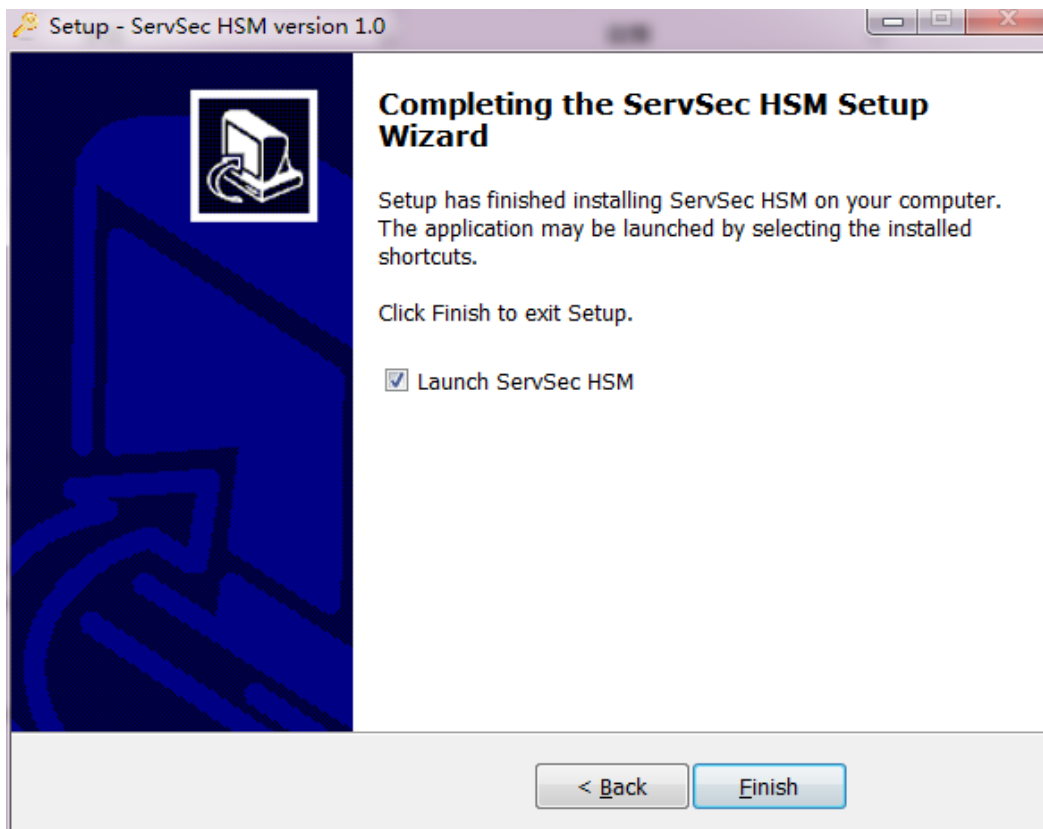
Click **【Install】**, installation will start, as shown below:



When installation finished, port configuration dialog will popup, as shown below:



Click **【Next】**, installation finished dialog will popup, as shown below:



Click **【Finish】**, installation finished.

4.2 Management tool connection

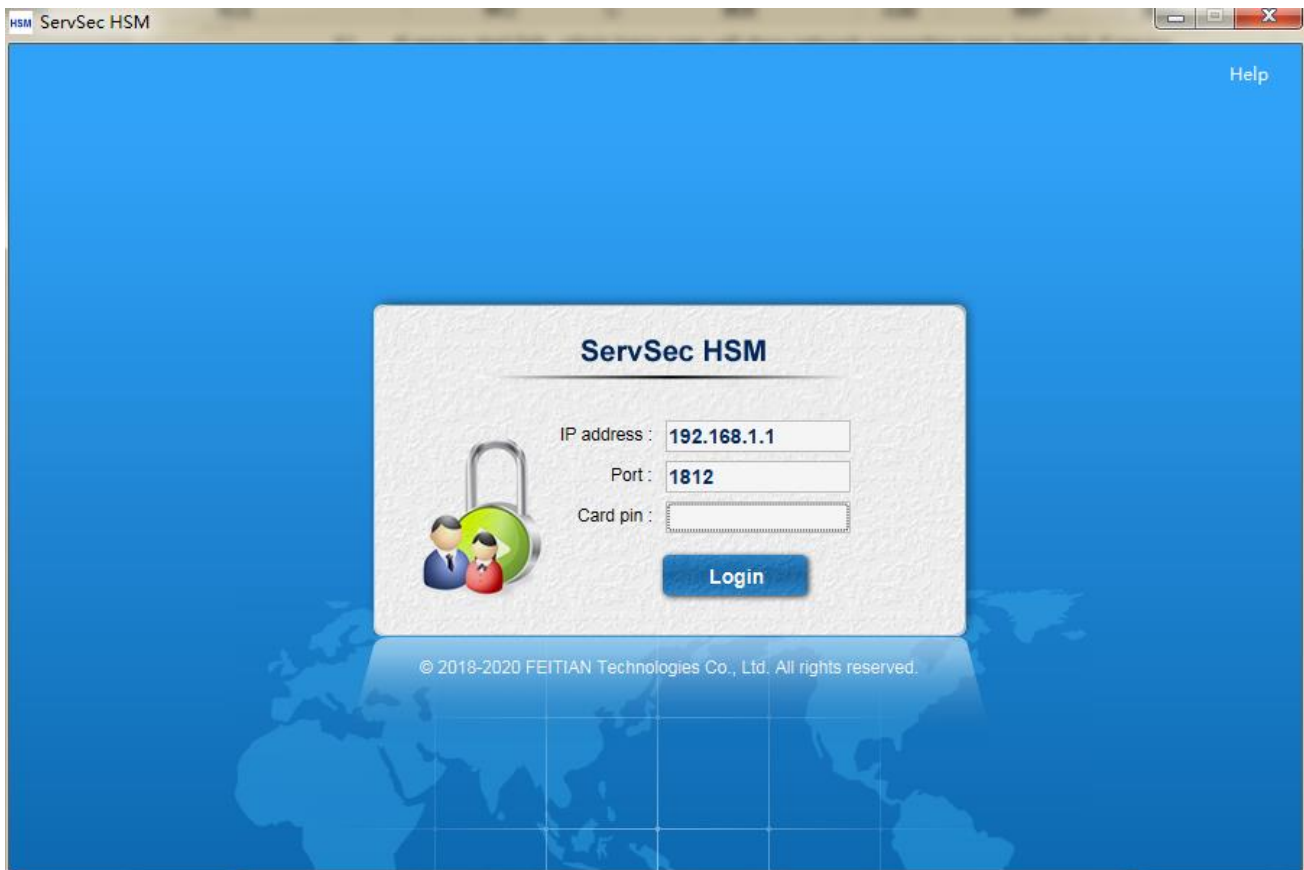
The users of management tool are System Manager, Safe Manager and Audit Manager, management terminal is connected to HSM via local network, the connecting procedures are:

- 1) After HSM service is started, click **【setting】** on touch screen, system manager authentication card authentication success, open setting page, click **【Tool IP Whitelist】** to configure, add the IP address of management terminal PC;
- 2) Manager install management tool on management terminal PC;
- 3) Ensure management terminal correctly connected within local network;
- 4) Manager open management tool, logon page will be displayed, default indication is HSM IP address and port to be connected, double check, if correct, then input Manager authentication card PIN to logon;

If service start fails, manager logon page will show “network connection error, logon fail”; if service starts successfully, then manager logon success and the manager can perform management operations

4.3 Logon/logout

After the HSM module is started, the management tool will load. Enter the correct information into the fields displayed on the touch screen. Insert the authentication card and input the PIN, then click **【Login】** to log in to the tool



Once logged in to the management tool, the manager can check current logon role in management tool's navigating bar. If no valid operation in 10 minutes, management tool will logout automatically. If operator want to use management tool again, he will need to insert manager authentication card and perform verification to logon again.

4.4 Manager Roles and Access Rights

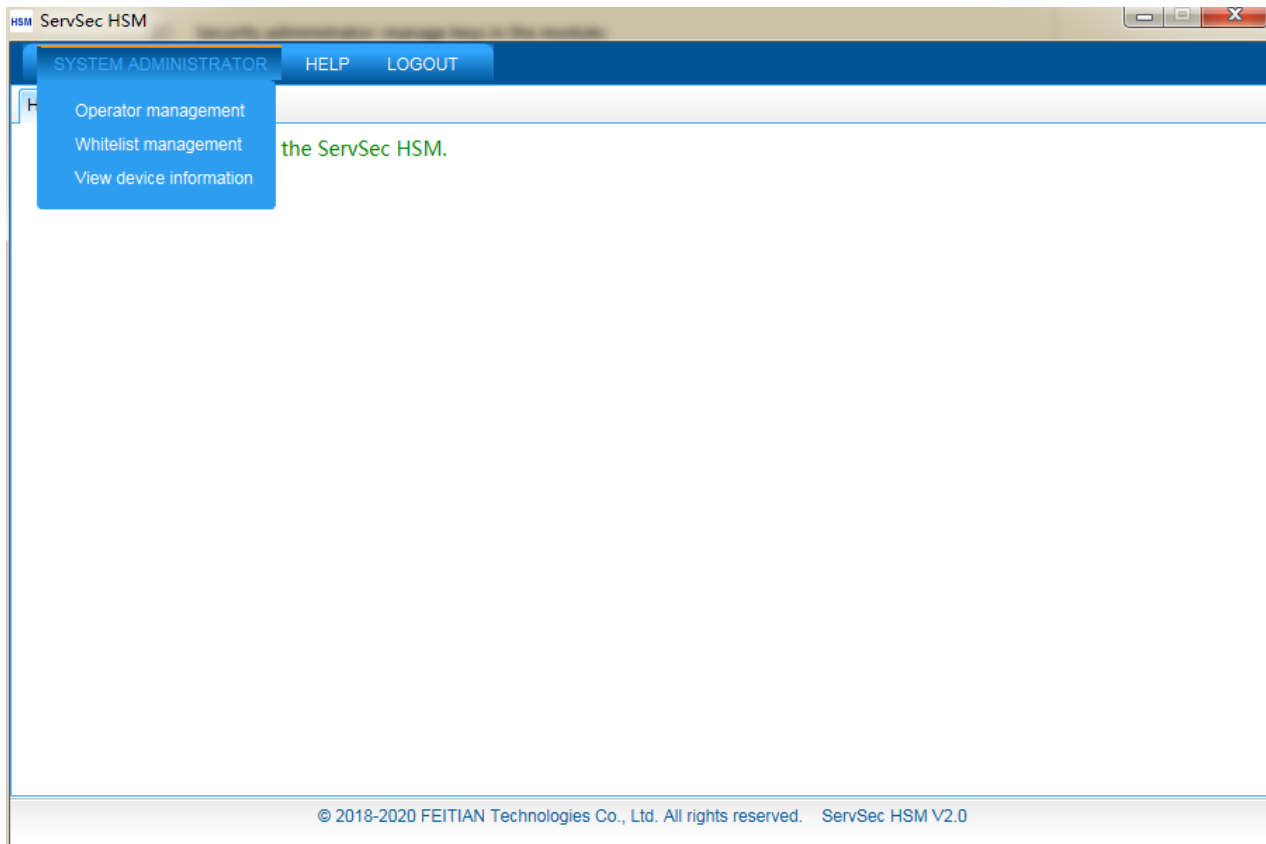
There are 3 manager roles: System Manager, Safe Manager and Audit Manager. Each role has an independent set of access rights.

- **System Manager:** The System Manager manages operators(user) who use the module's services (operating system).
- **Safe Manager:** The Safe Manager manages the keys in the module for security.
- **Audit Manager:** The Audit Manager manages the log records for the module.

When logged in to the management tool, the manager needs to insert their authentication card and input the PIN for verification.

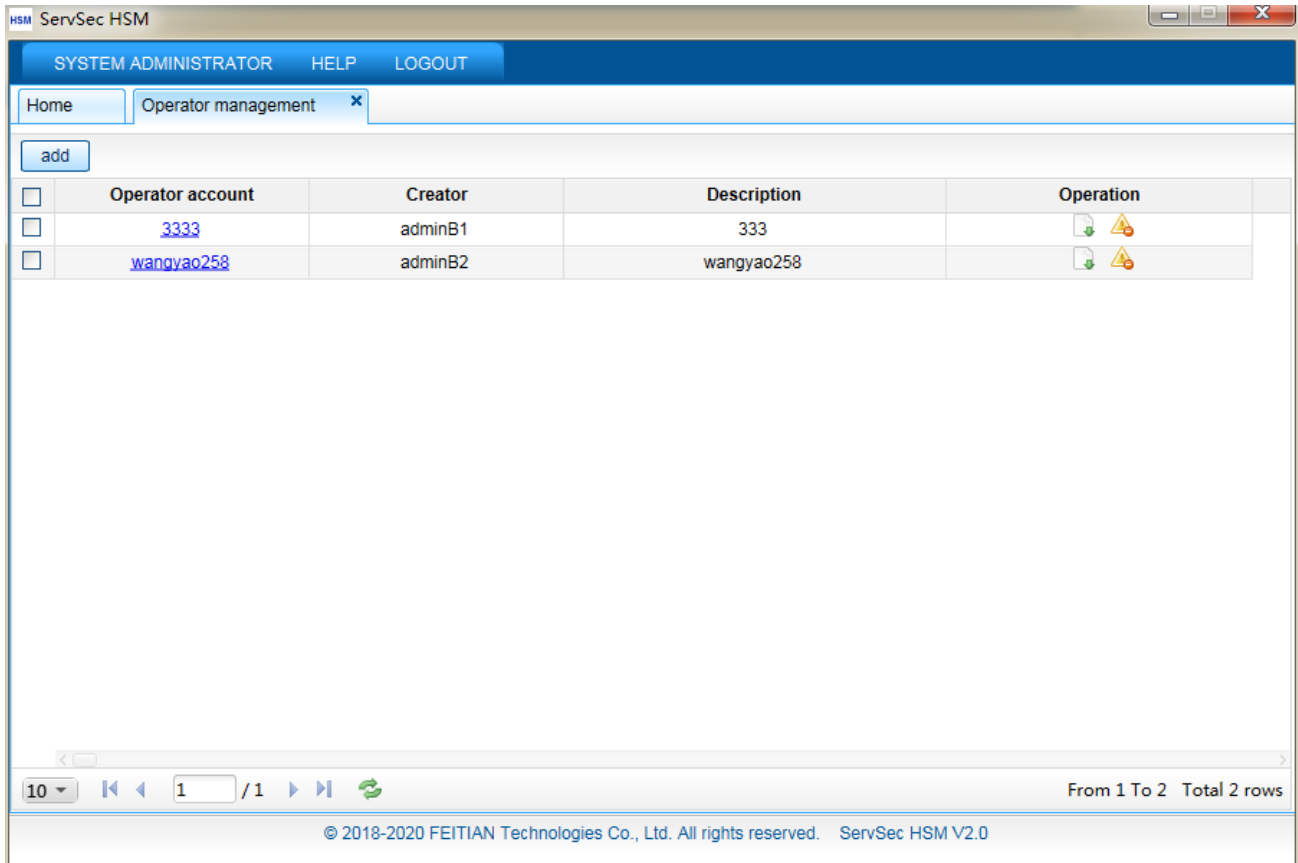
4.4.1 System Manager

After logging in, open the **【SYSTEM ADMINISTRATOR】** menu to view System Manager management rights.



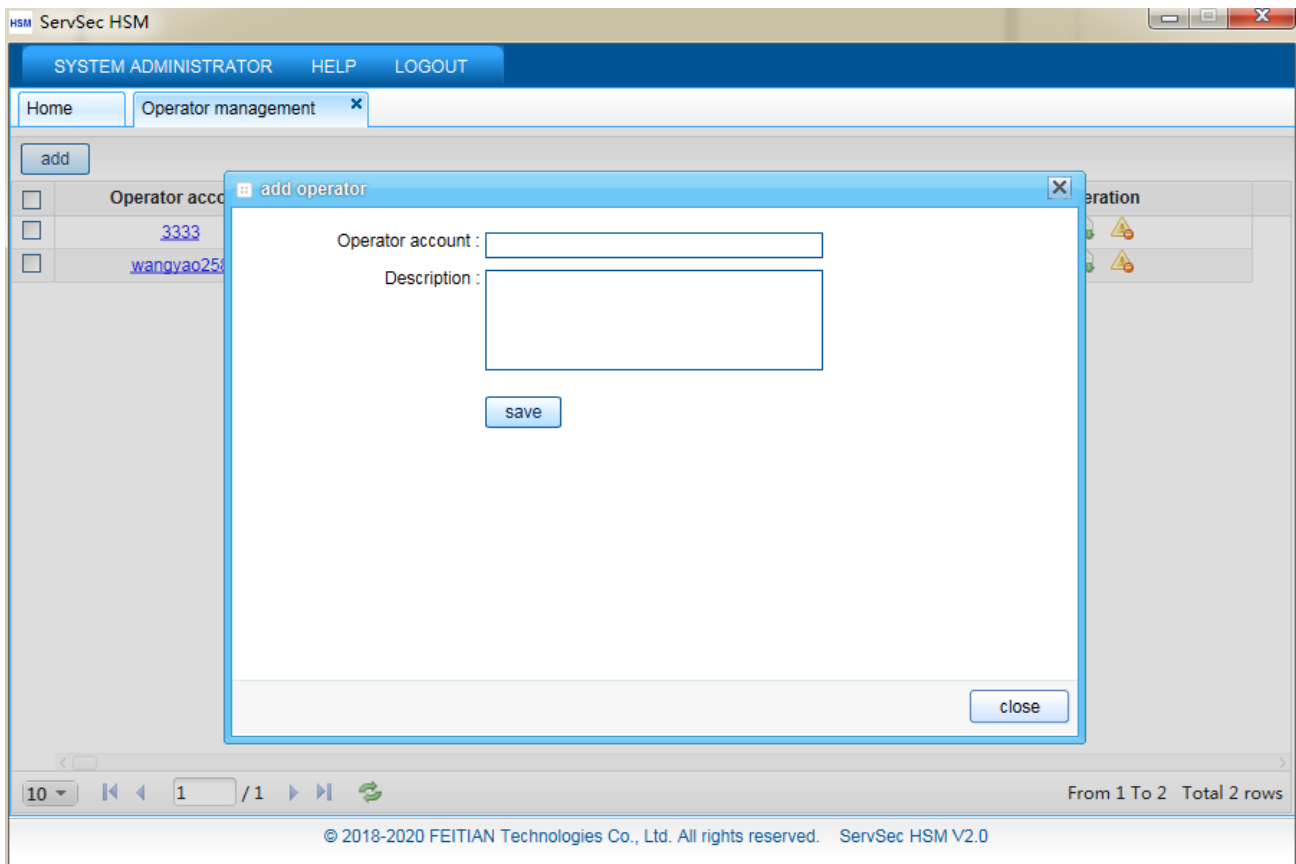
4.4.1.1 Operator management

Operator Management manages all operators, or users, for the module. It can add, delete, and check operators, reset operator keys, and download license files. All operators will be displayed in the Operator Management tab.






Add operator

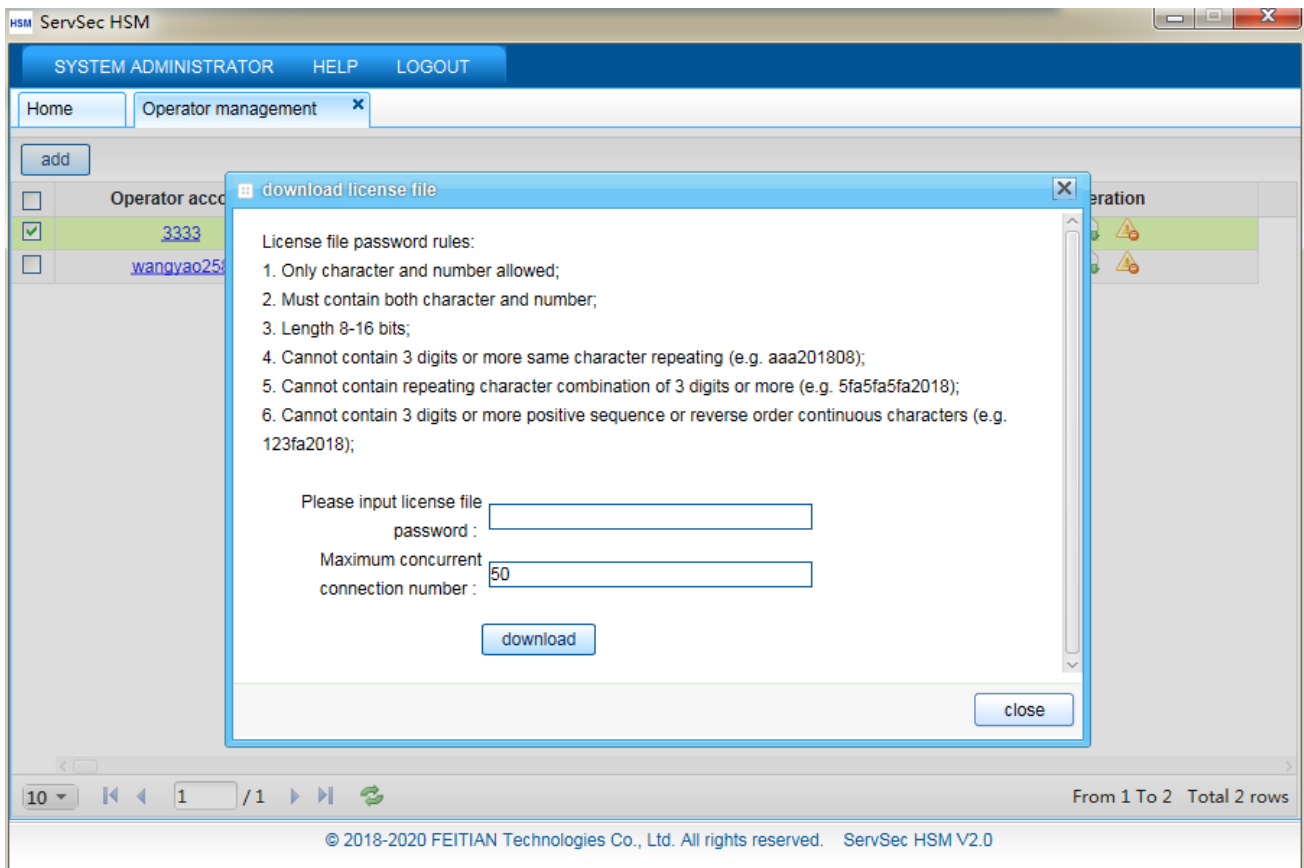
Click **【add】**, adding operator box will popup, input operator name and description, click **【save】**, saved as shown in the figure below:





Download operator key


Operator account	Creator	Description	Operation
3333	adminB1	333	 

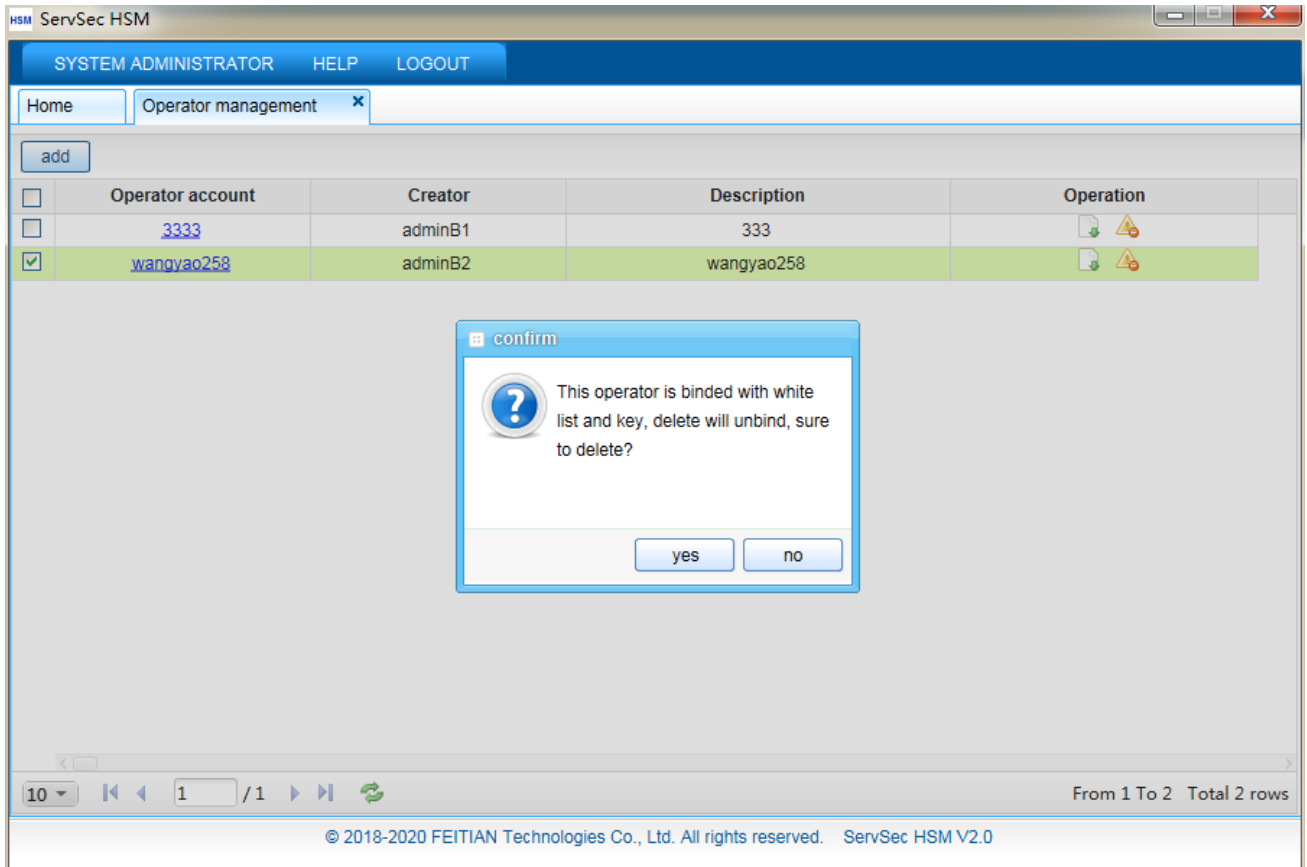
Click  **【download license file】** in operating row of an operator's data. Download box will appear. Input PIN and maximum number of concurrent connections, then click **【download】**. License file can be downloaded to directory of your choice as shown in the figure below:



Delete operator

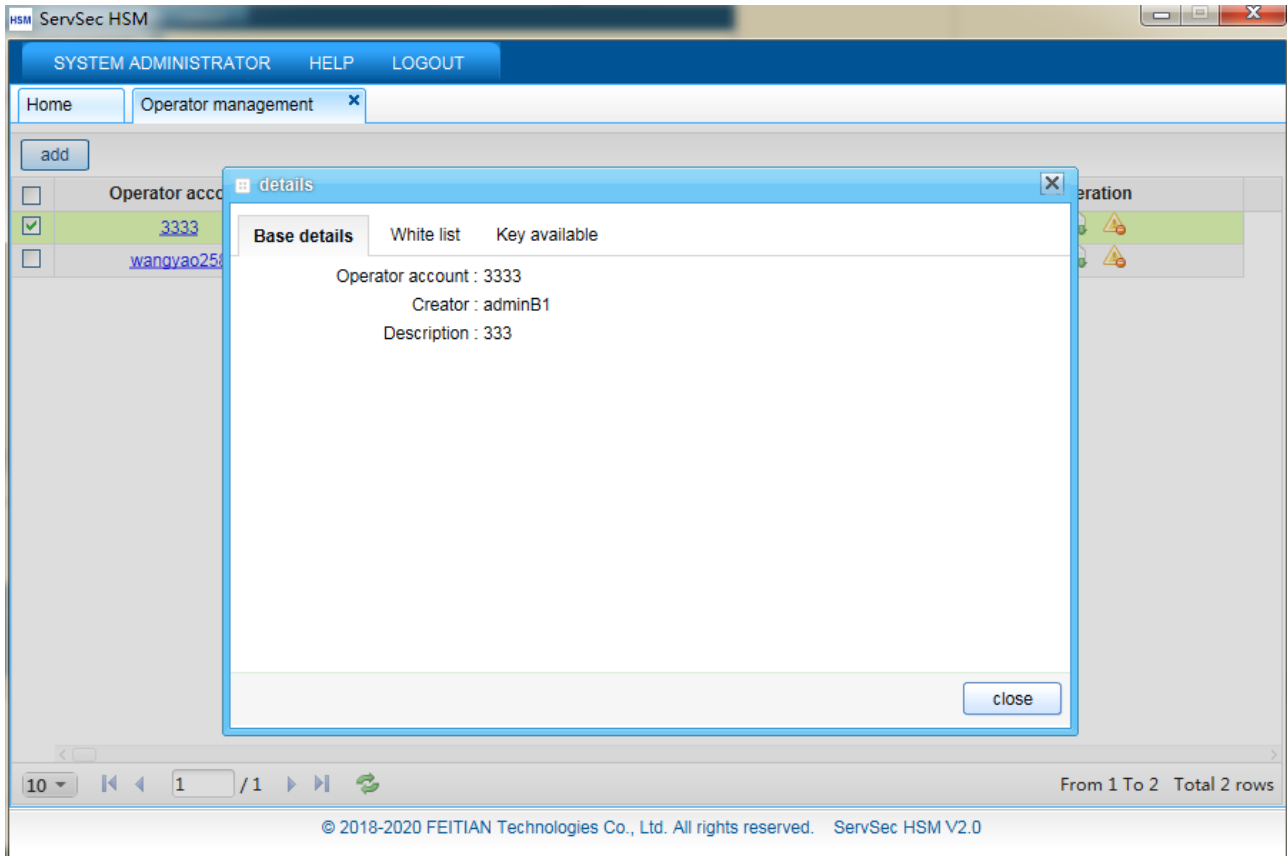
Operator account	Creator	Description	Operation
3333	adminB1	333	 

Click  **【delete】** in operating row of an operator's data. The delete confirmation box will appear. Click **【yes】** to delete the operator along with the IP data bundled in IP white list. After delete operation, the application system will ban this operator from performing any operation.



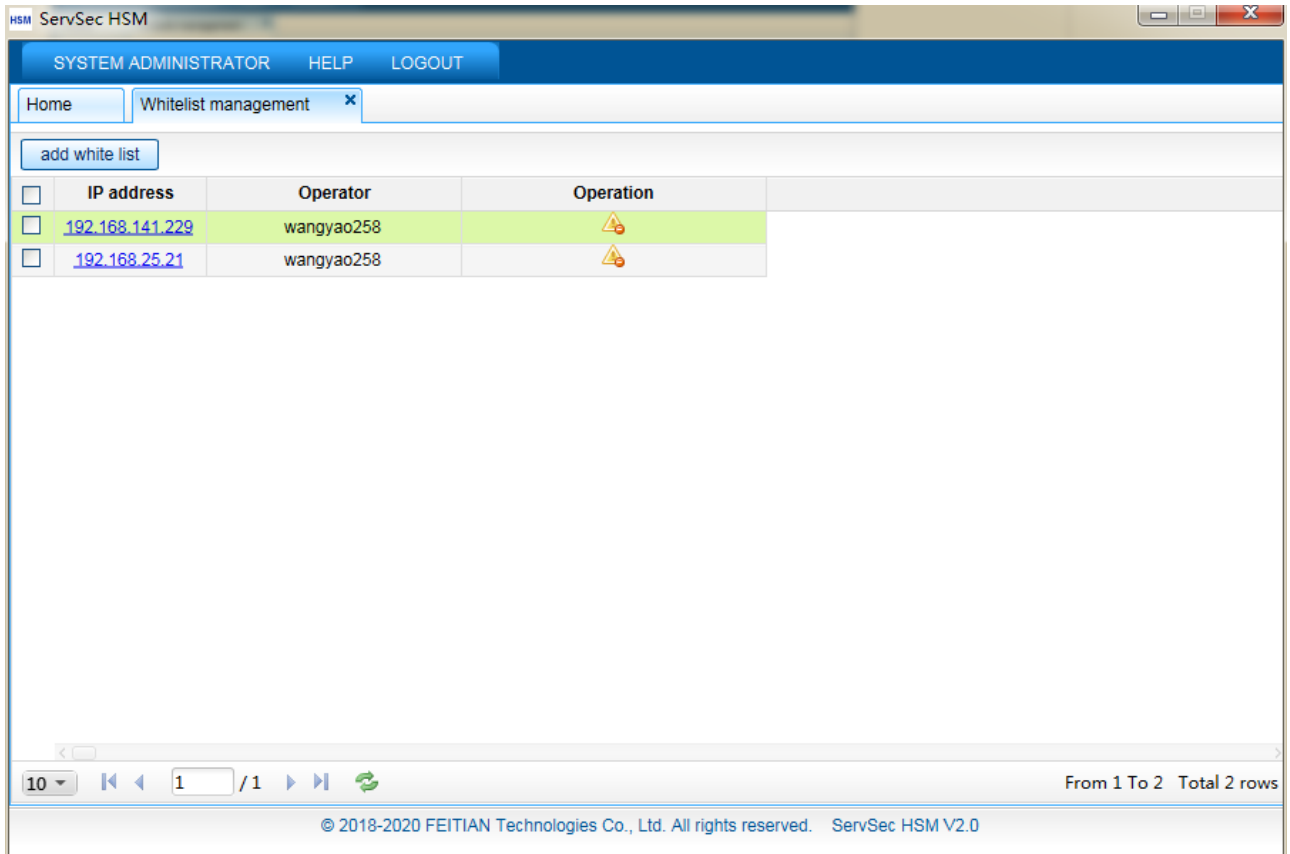
Check detail information

Click operator account to check basic information, IP white list, and keys available for the operator, as shown in the figure below:



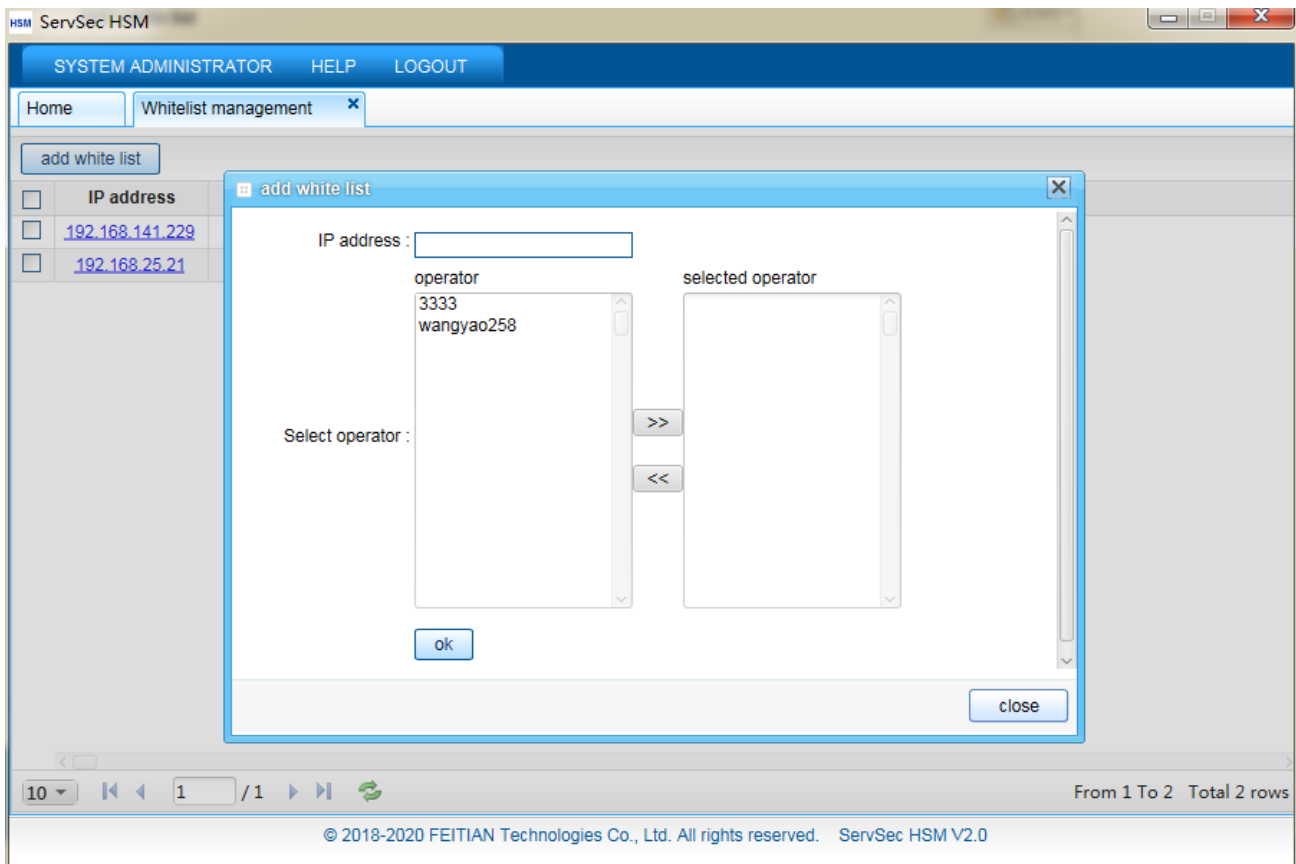
4.4.1.2 White list management

This function can manage the white list. Only IPs already existing in the white list can have the right to access services provided by the module. Click the **【Whitelist management】** tab to show the current white list, as shown in the figure below:



Add white list

This function is mainly for adding IP addresses to the white list. Click **【add white list】**, then input the IP address you want whitelisted. Select one or more operators, then click **【ok】** to finish adding the IP address to the whitelist:



Note : If the operator has not been added with the IP addresses listed in the white list, the operator will be banned from accessing HSM services.

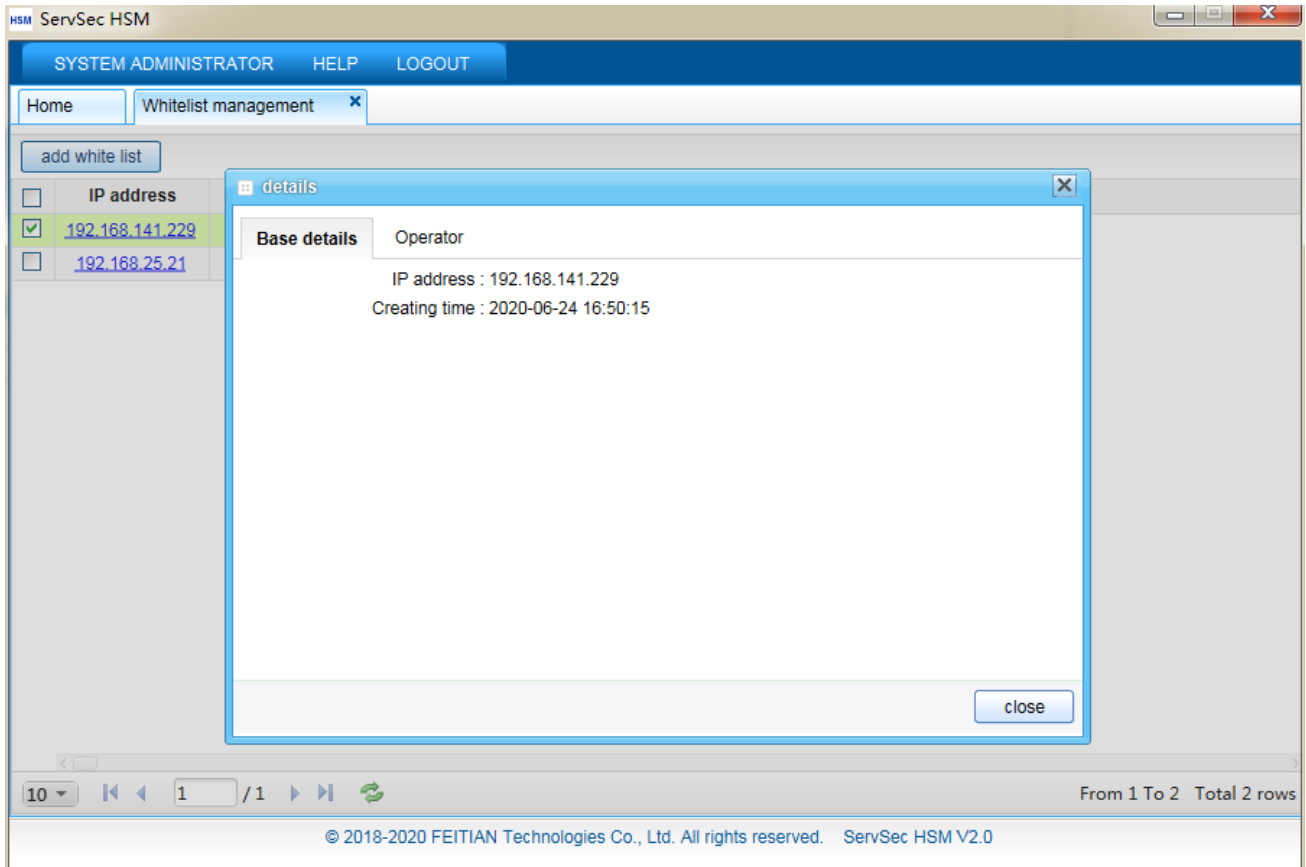
Delete white list

IP address	Operator	Operation
192.168.25.81	test	

This function can delete IP addresses in the white list. Click to delete the selected IP address and click **【yes】** to confirm. The IP address will be deleted and its binding with the operator will be released.

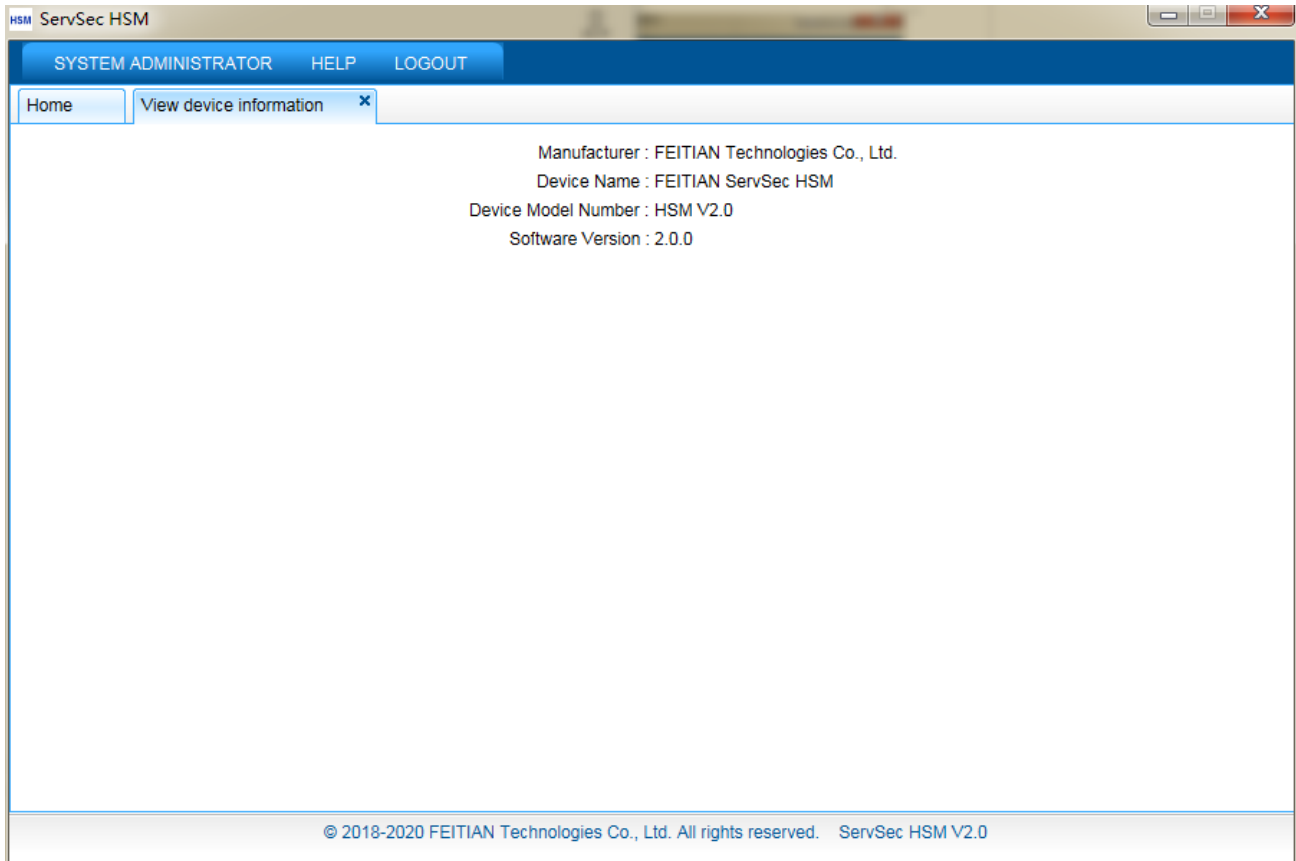
Check detail information

This function allows you to check detailed IP information. Click any IP address in the white list and the detailed information of that IP will appear. The operator can find this IP address and the operator bundled with this IP, as shown in the figure below:



4.4.1.3 View device information

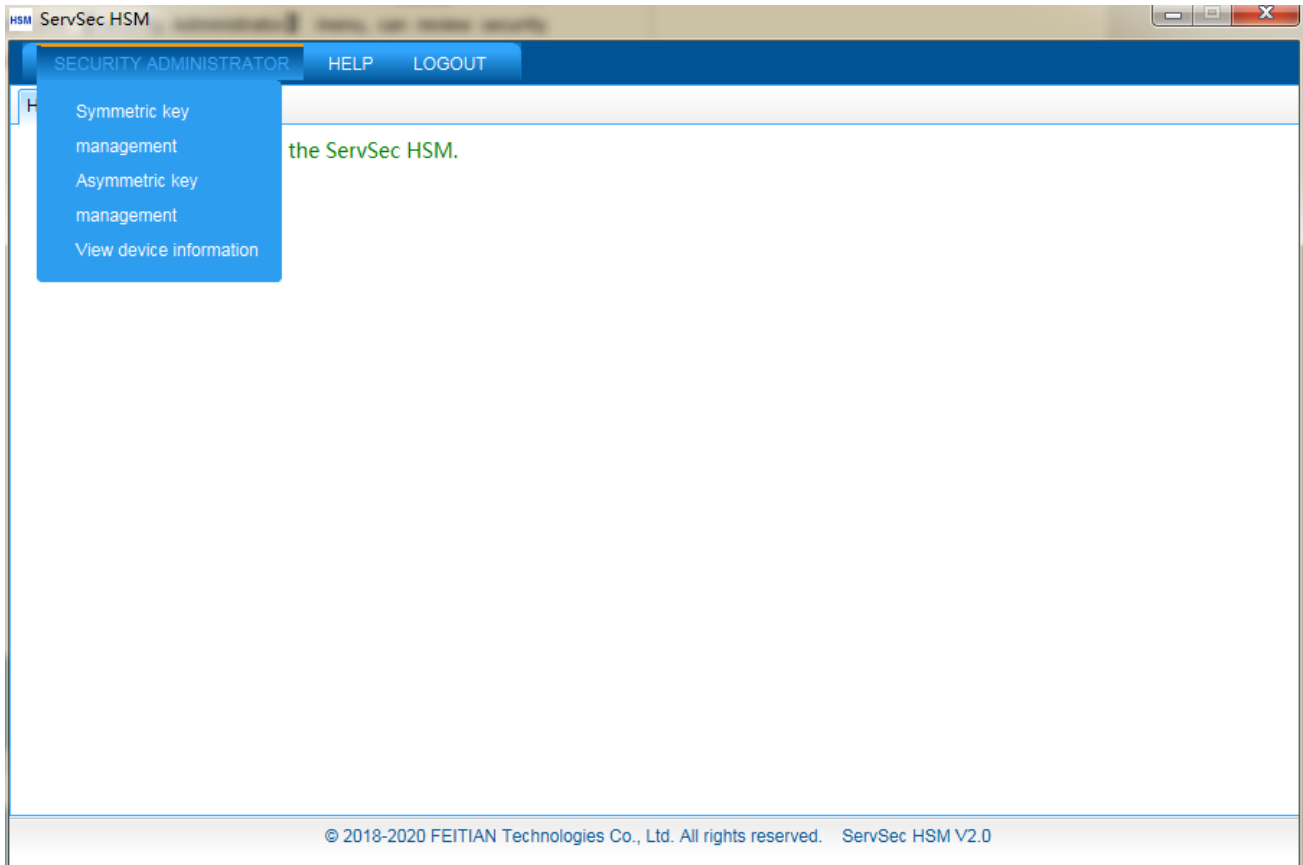
This function allows you to check the device information. Click **【View device information】** in the System Manager menu list. show current device info, including device manufacturer, product name, model, etc., as shown in the figure below:



4.4.2 Safe Manager

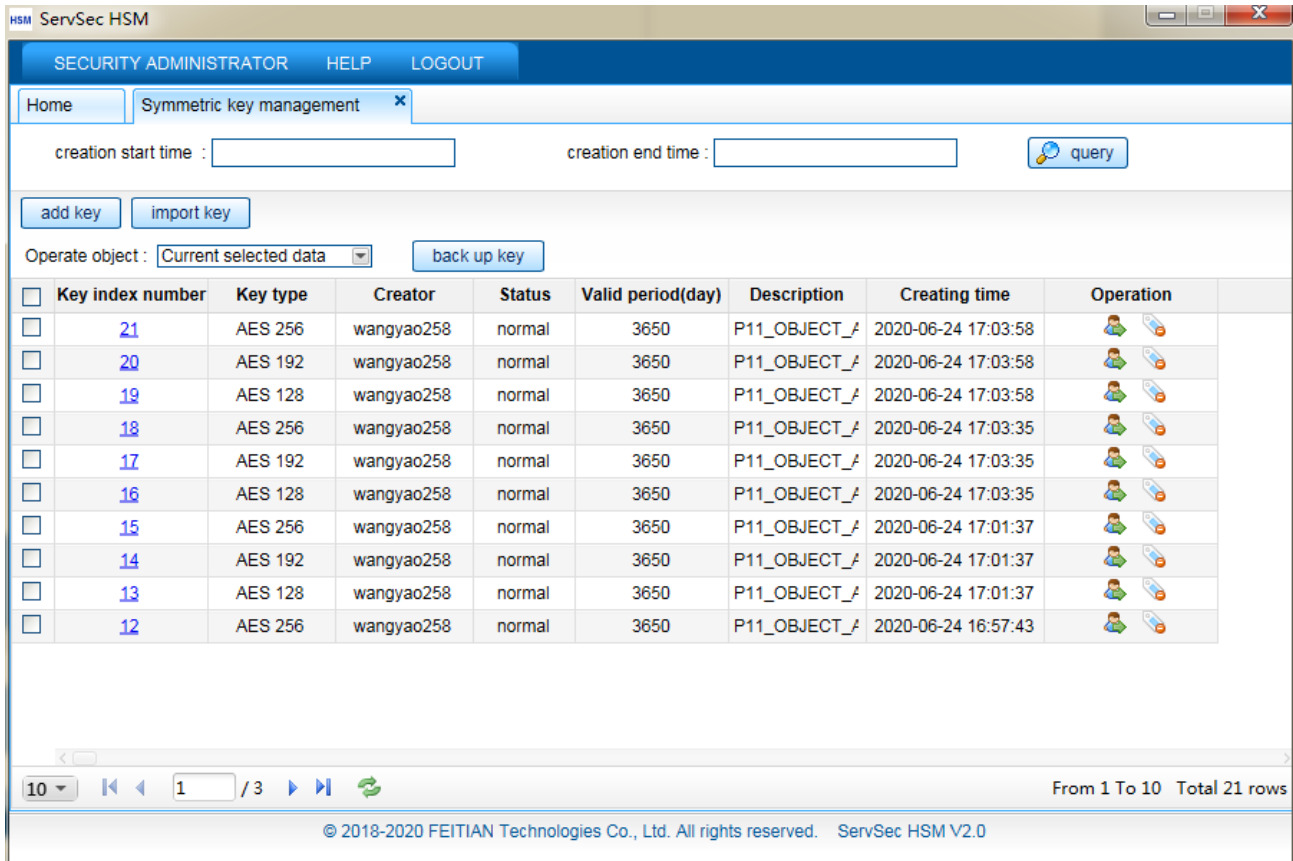
The Safe Manager mainly manages the keys in the module, including symmetric/asymmetric key adding, importing, exporting, deleting and binding with operators;

Click the **【Security Administrator】** menu to review the Safe Manager function list, as shown in the figure below:



4.4.2.1 Symmetric key management

This function mainly manages symmetric keys. It can implement add/import/export/delete key and binding operator process. Click **【Symmetric key management】** in the Safe Manager menu list, show symmetric key management page, as shown in the figure below:

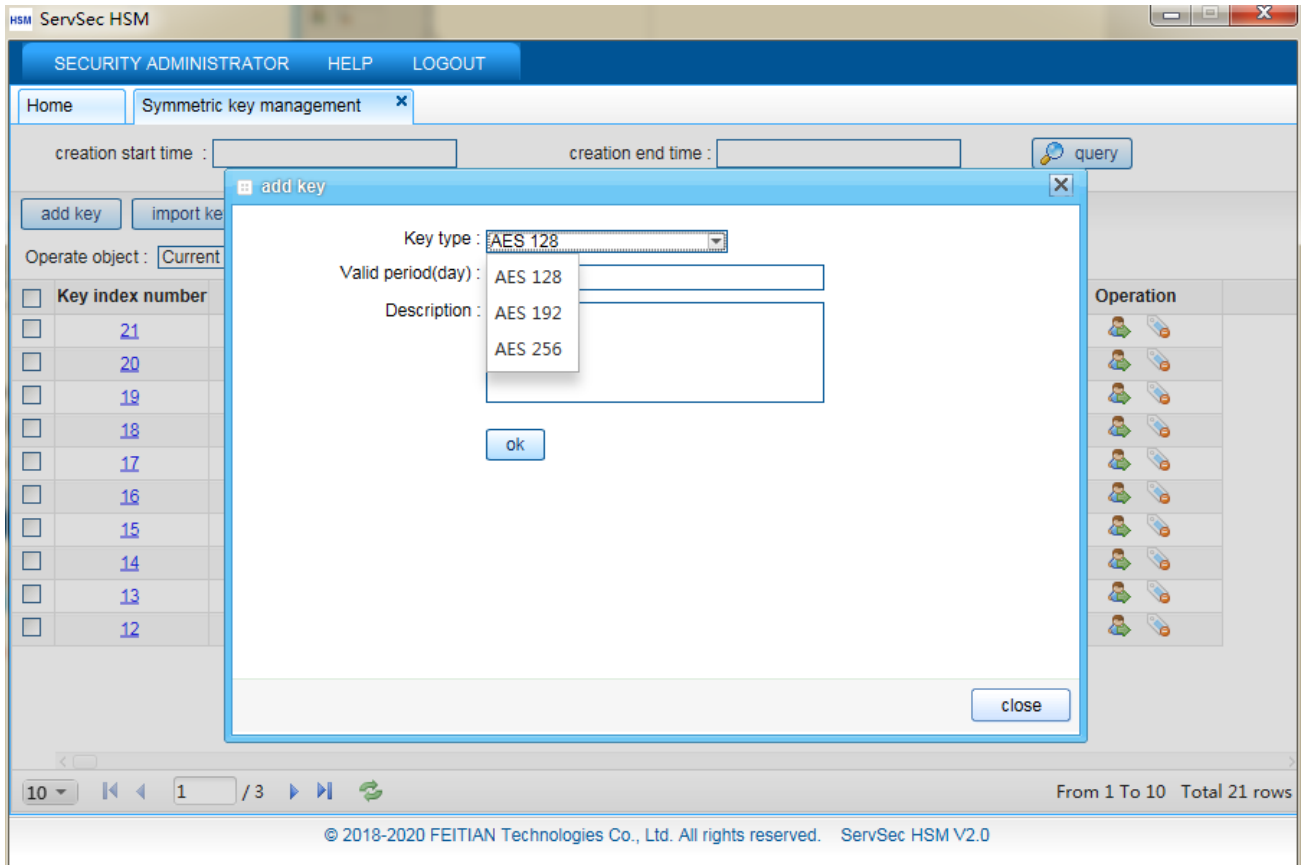


Key query

Select the start and end time of the creation, and click **【query】** to query all the key data in the selected time interval.

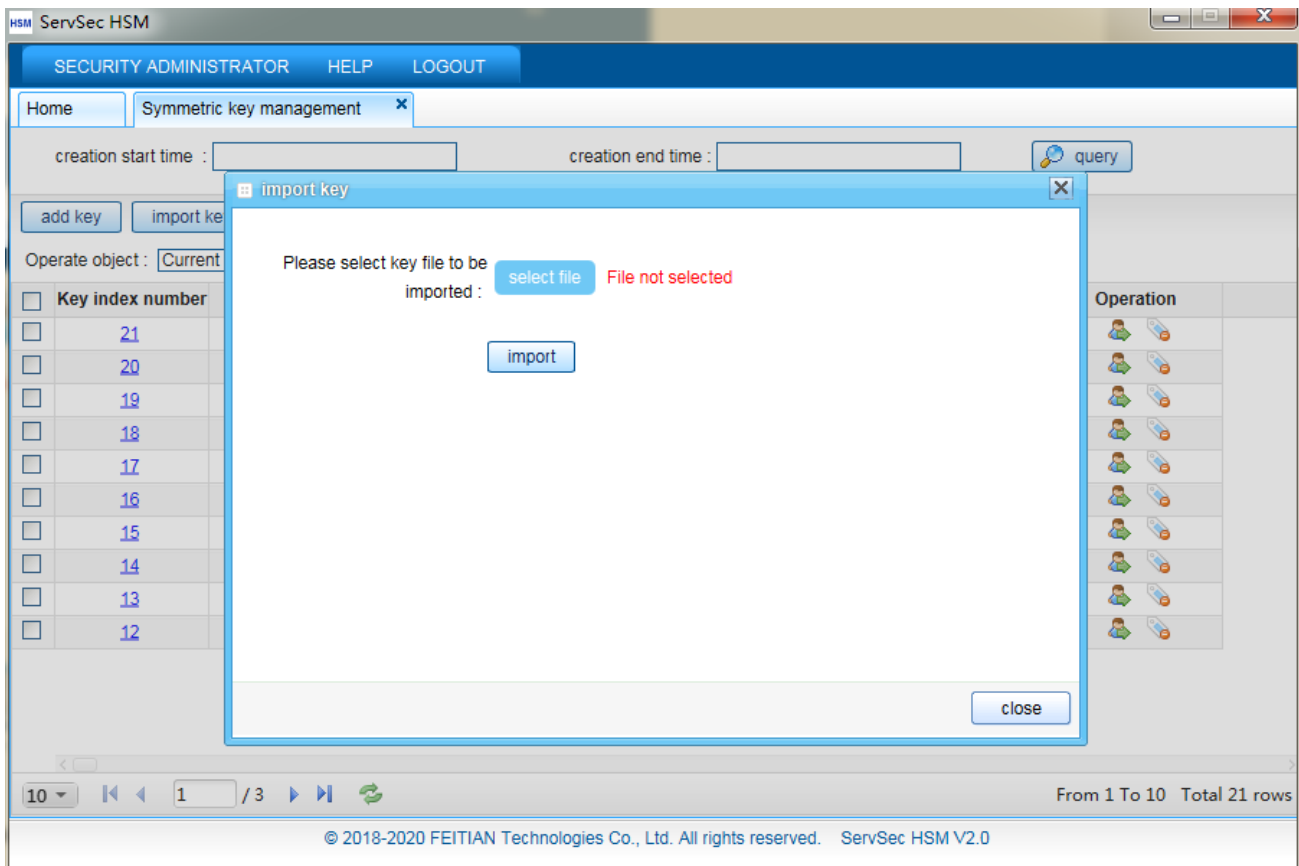
Add key

This function is mainly for adding symmetric keys. Click **【Add key】** in the symmetric key management page and an Add Key window will appear. Input corresponding key information, click **【ok】**, this key data will be added. The adding key page is shown in the figure below:



Import key

This function can batch import symmetric keys, click **【Import key】** in symmetric key management page, import key box will popup, click **【chose file】**, browse and select local key files, click **【import】**, can import all key data within this file. Key import page is shown in the figure below:



Key back up

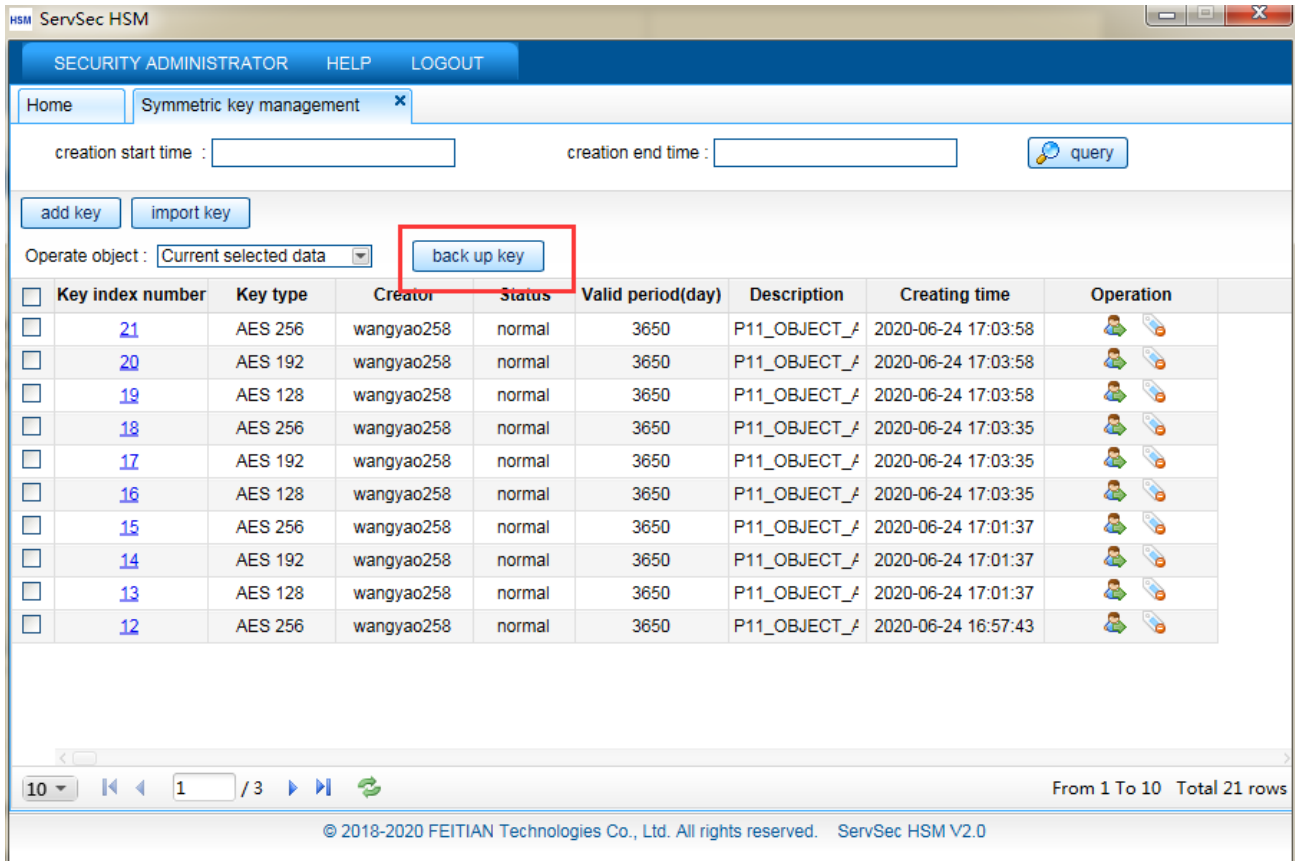
This function can back up symmetric key data to a local hard drive.

First method:

Select one or more symmetric key data to be exported, set the operation object to "Current selected data", click **back up Key**, pop up the prompt box, and click **Yes** to back up the selected key to the specified directory.

Second method:

After inputting query conditions for query, set the operation object to "Current query data", click **back up key** in symmetric key management page, click **yes** when the confirmation dialogue box appears. Query keys will be backed up to specified directory.



Discard/restore keys

Key index number	Key type	Creator	Status	Valid period(day)	Description	Creating time	Operation
21	AES 256	wangyao258	normal	3650	P11_OBJECT_#	2020-06-24 17:03:58	
20	AES 192	wangyao258	discard	3650	P11_OBJECT_#	2020-06-24 17:03:58	

This function can discard or restore specified symmetric key data.

Discard: click in specified symmetric key data operating column to set this key data to discarded status.

Restore: click in specified symmetric key data operating column to set key data to normal status.

Note: Any key that has expired is automatically updated to be invalid. Any key data that is automatically invalidated cannot be recovered.

Bind/unbind operator

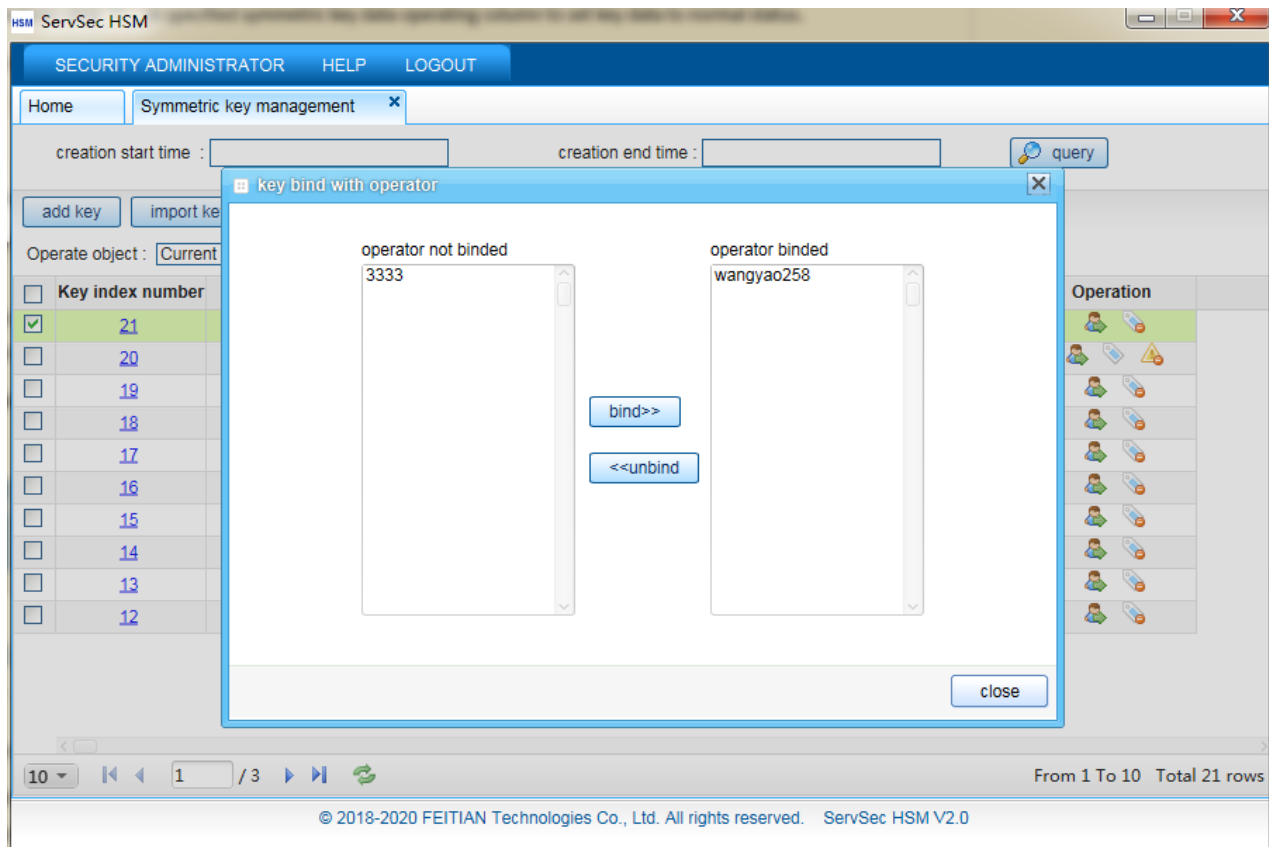
Key index number	Key type	Creator	Status	Valid period(day)	Description	Creating time	Operation
21	AES 256	wangyao258	normal	3650	P11_OBJECT_#	2020-06-24 17:03:58	

This function can bind an operator to a symmetric key. Click **【key bind with operator】** in symmetric key data operating column of the operator to be bound with.

When the dialogue box appears, the following operations are available:

Binding: select one or more operators and click **【bind】**. Only after being bound with a given key data can the operator perform crypto service using the bound key.

Unbinding: select one or more operators and click **【unbind】** to unbind key data with the selected operators.



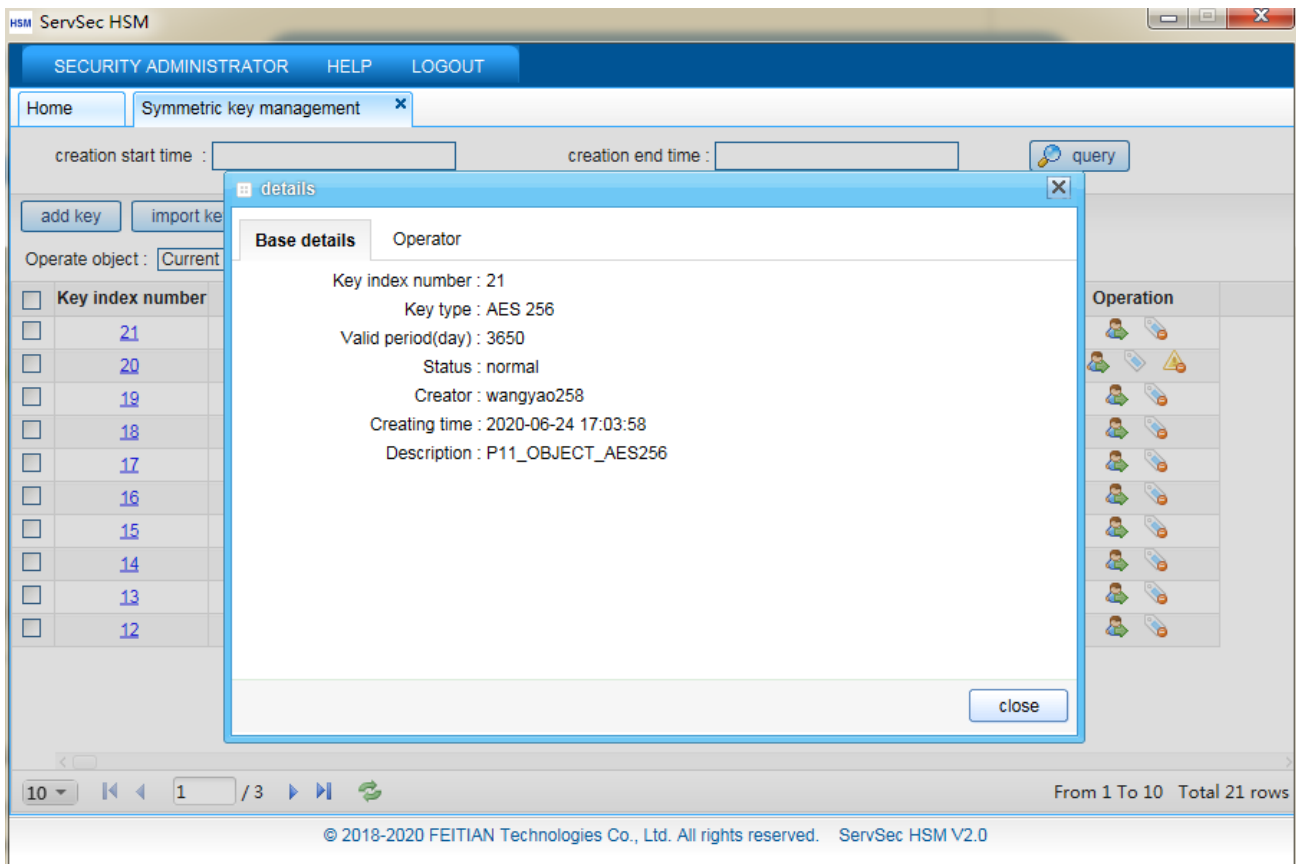
Delete key

Click  in the invalid key data operation column then click **【yes】** to confirm the deletion.

Note: Only key data in the invalid state can be deleted.

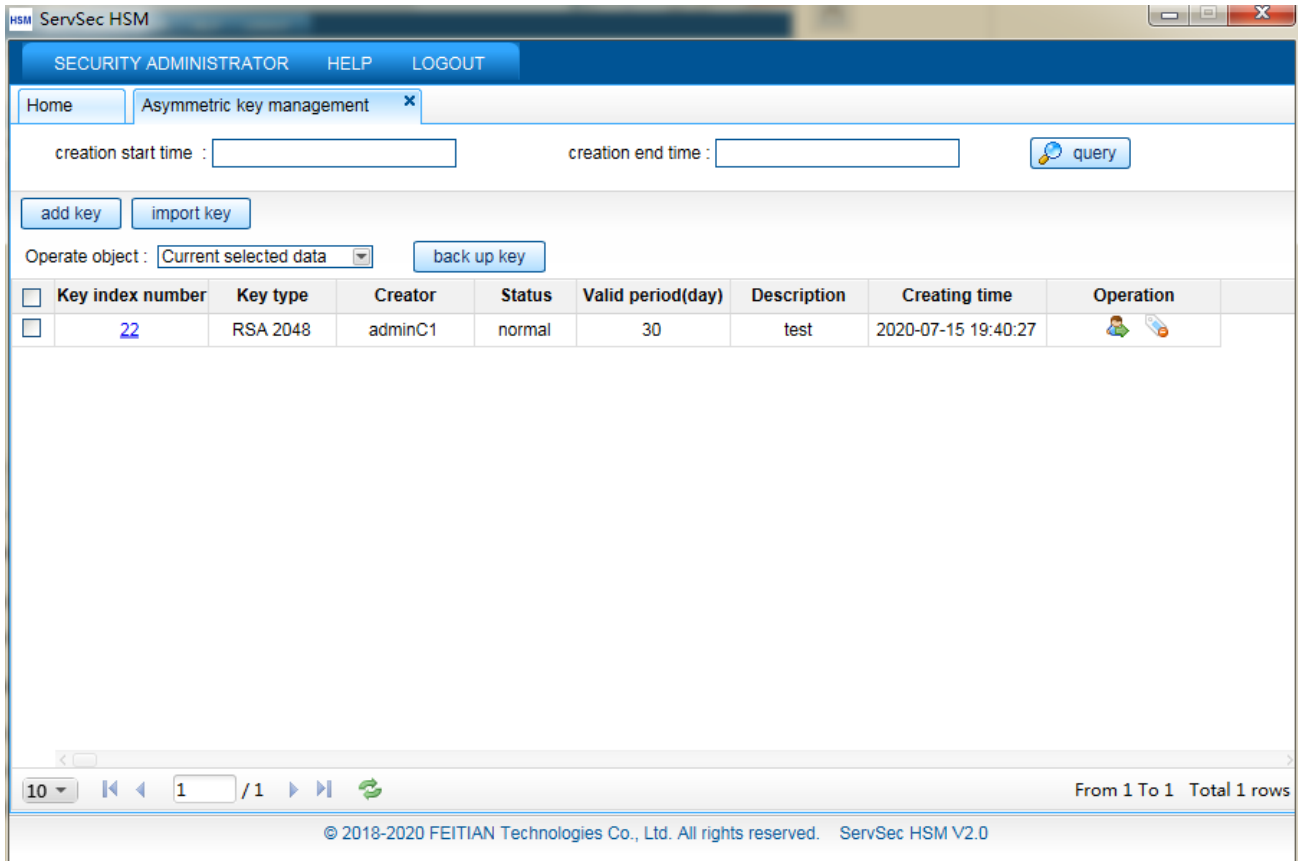
Check key detail information

This function lets you review detailed information of keys. To do so, click **Key Index** to open the key detail information box.



4.4.2.2 Asymmetric key management

This block of functions is mainly used to manage asymmetric keys (RSA1024, RSA2048, ECC), can perform add/import/export/delete keys, and bind operators. Click **【Asymmetric key management】** in the Safe Manager menu, show asymmetric key management page, as shown in the figure below:

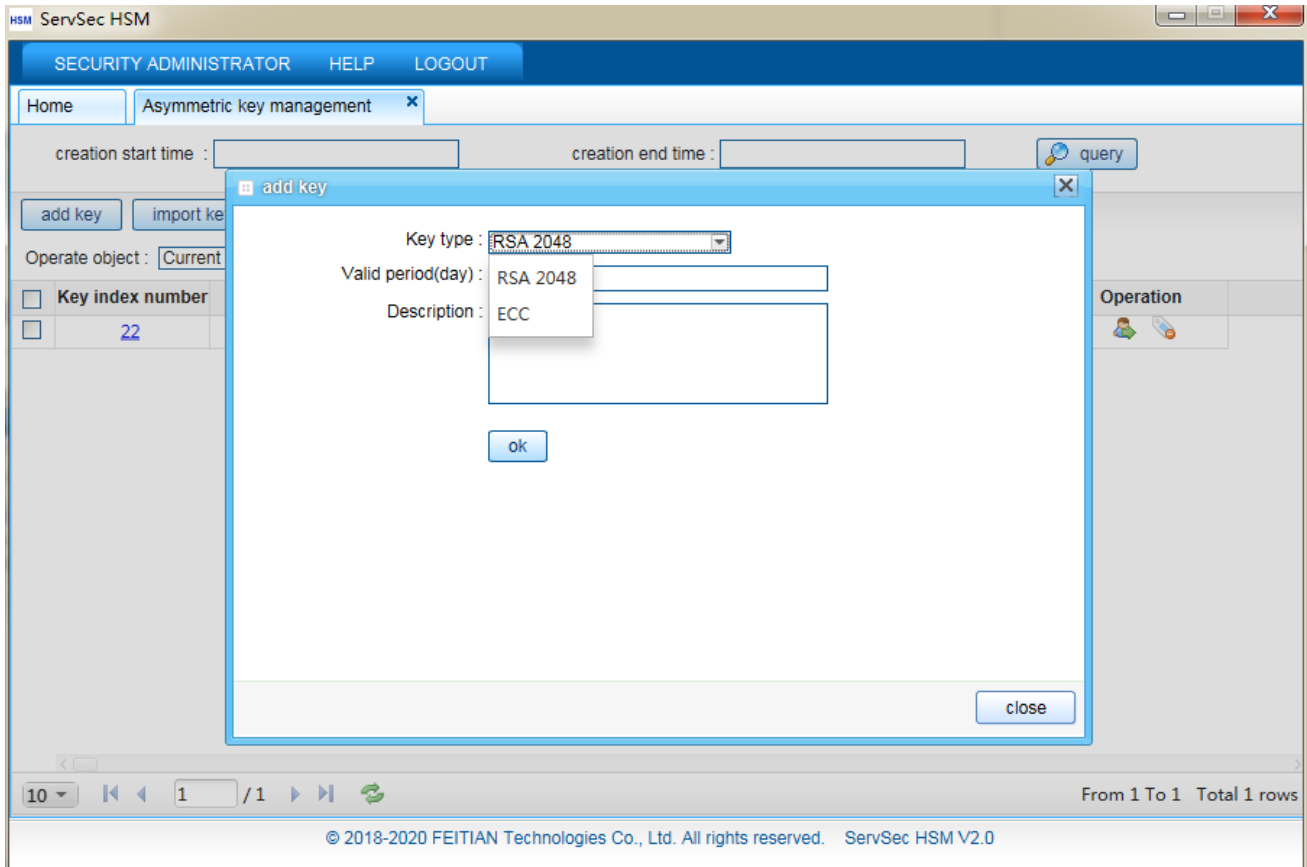


Key query

Select the start and end time of the creation and click **【query】** to query all the key data in the selected time interval.

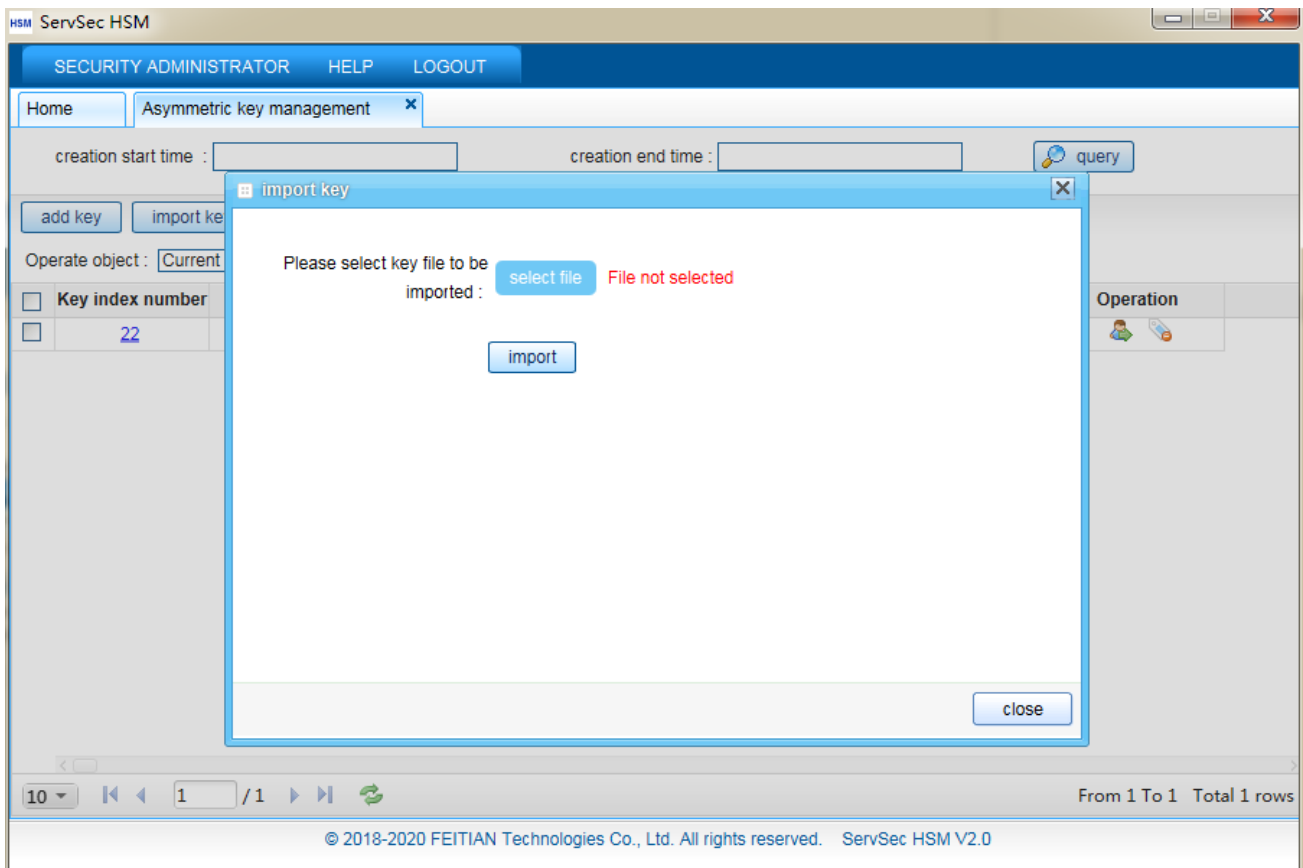
Adding keys

This function mainly allows adding asymmetric keys. Click **【Add key】** in the asymmetric key management tab, then input the corresponding key data. Click **【ok】** to finish adding the key data.



Importing key

This function can batch import asymmetric keys, click **【Import key】** in asymmetric key management page, import key dialog box will popup, click **【chose file】** to browse and select local key files, click **【import】**, can import all key data in the file. The page of key importing function is shown in the figure below:



Back up key

This function can back up the asymmetric key data to a local drive. There are two methods of doing so.

Method 1

Select one or more asymmetric key data to be exported, set the operation object to "Current Selection Data", click **back up Key**, pop up the prompt box, and click **Yes** to back up the selected key to the specified directory.

Method 2


After inputting query conditions for query, set the operation object to "Current query Data", click **back up key** in asymmetric key management page, popup dialog box, click **yes**, query keys will be backed up to specified directory.

Discard/restore keys

Key index number	Key type	Creator	Status	Valid period(day)	Description	Creating time	Operation
23	ECC	adminC1	normal	30	test	2020-07-15 19:41:36	
22	RSA 2048	adminC1	discard	30	test	2020-07-15 19:40:27	



This function can discard or restore specified asymmetric key data.


Discard: click in specified symmetric key data operating column to set this key data to discarded status.

Restore: click  in specified asymmetric key data operating column to set key data to normal status.

Note: The key that has expired is automatically updated to be invalid. The key data that is automatically invalidated cannot be recovered.

Bind operator

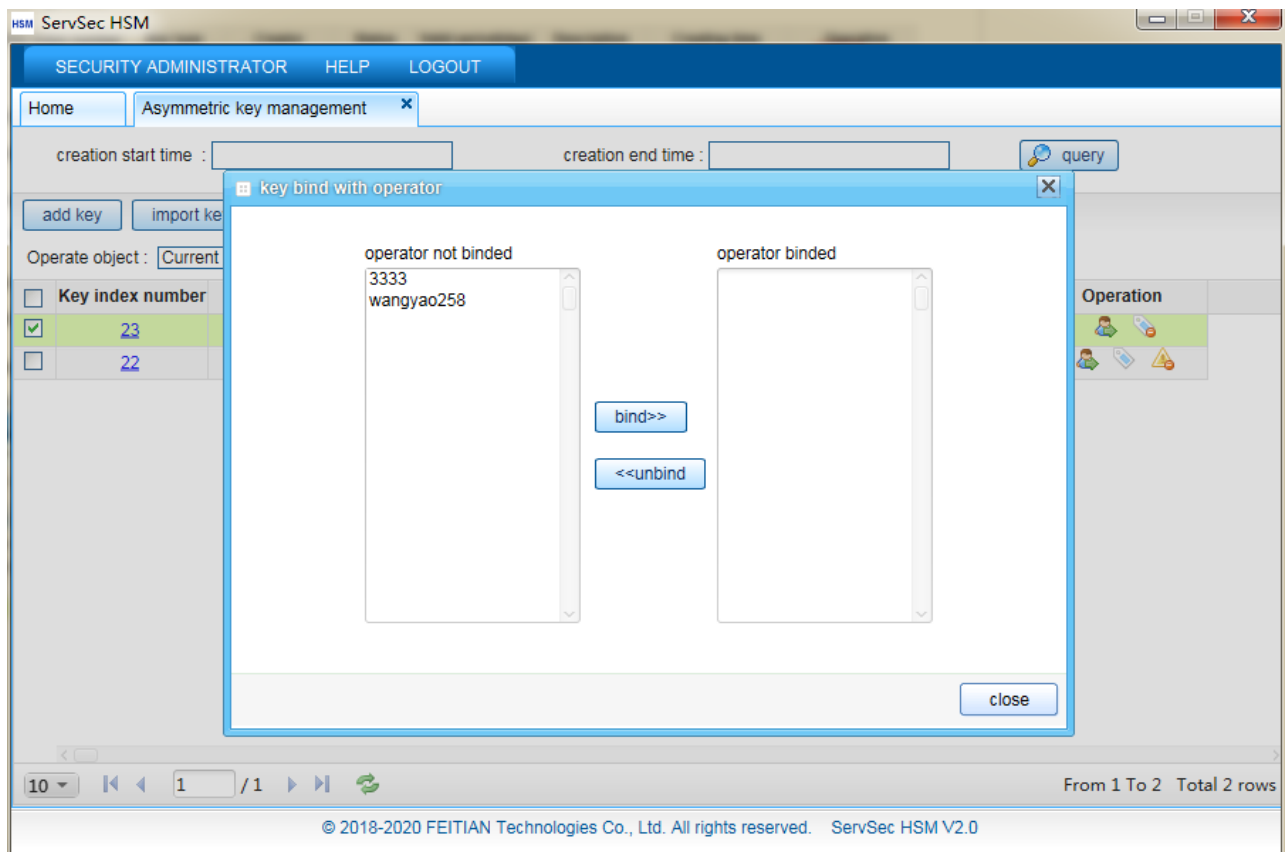
Key index number	Key type	Creator	Status	Valid period(day)	Description	Creating time	Operation
23	ECC	adminC1	normal	30	test	2020-07-15 19:41:36	 

This function can bind operator for asymmetric keys. Click  **【Key bind with operator】** in asymmetric key data operating column of operator to be bound with, key bind box will popup;


Bind: select one or more operators, click **【bind】**, bind success, only when the key is bound with the operator, the operator can use the bound key perform crypto operation.

Unbind: select one or more operators, click **【unbind】**, unbind success, the key data will be unbound with operators.

Key bind with operator page is shown in the figure below:



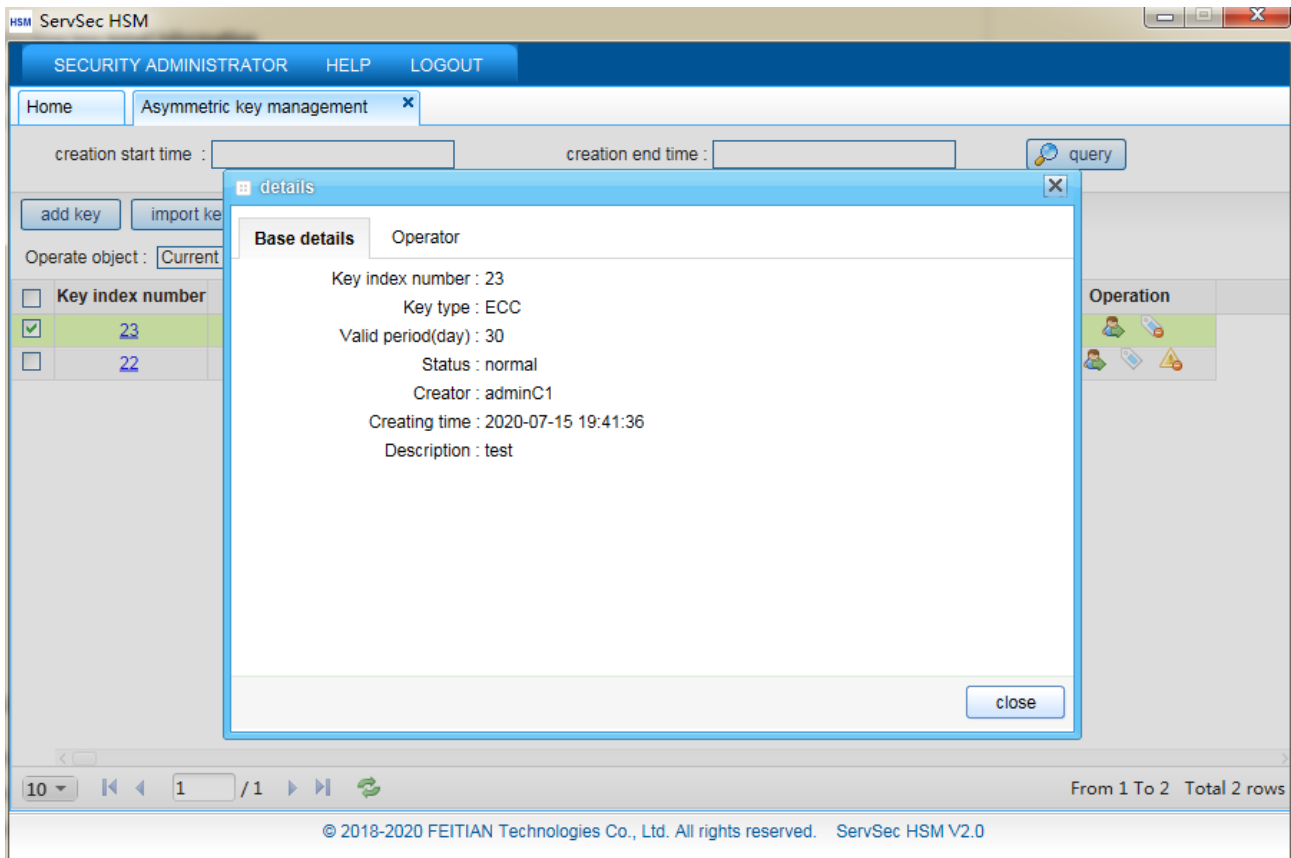
Delete key

Click  in the invalid key data operation column. The Delete Confirmation window will appear. Click **【yes】**. The key data can be deleted.

Note: Only the key data in the invalid state can be deleted.

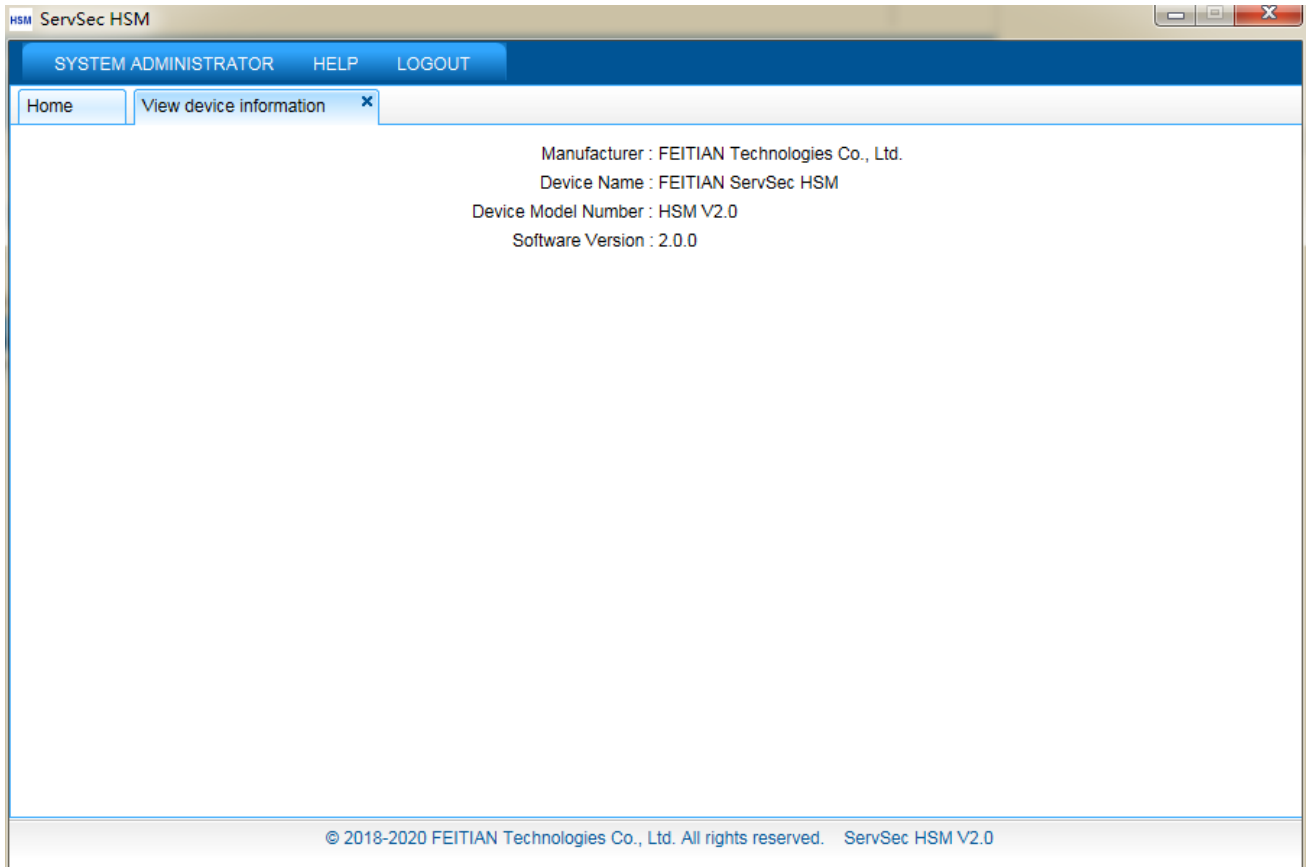
Checking key detail information

This function supports key detail information checking. Click key index for the key detail window to appear, as shown in the figure below:



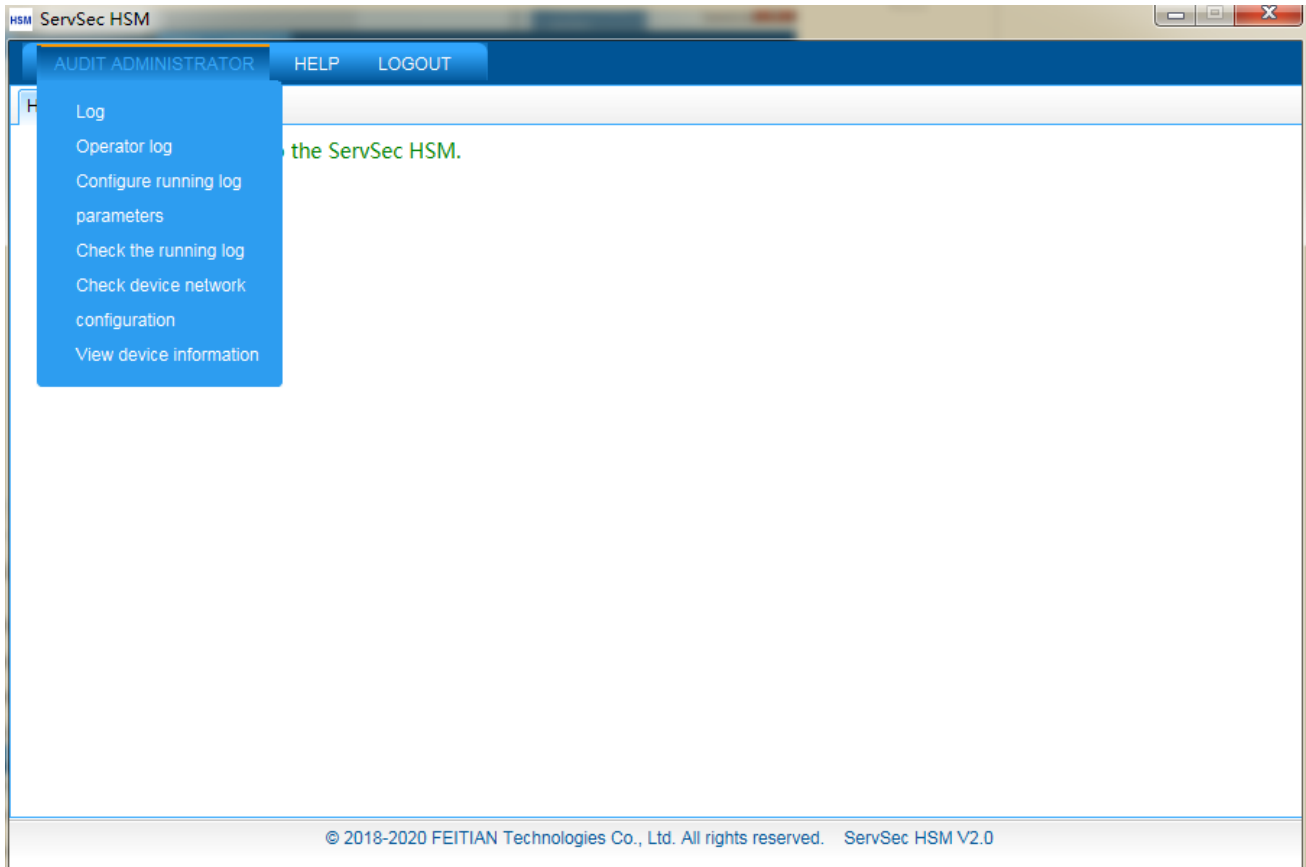
4.4.2.3 View device information

To check device information, click **【View device information】** in the Safe Manager menu list:



4.4.3 Audit Manager

Audit Manager is mainly in charge of reviewing operation log of all managers and operators, setting retaining days and file size of audit log files. Click **【AUDIT ADMINISTRATOR】** to check Audit Manager functions list, as shown in the figure below:



4.4.3.1 Logs

This block of functions support manager log files inquiry and checking. Operator can check and export specified log files of given manager according to log files' starting and ending time. Click **【Log】** in Audit Manager menu list, enter manager operating page, as shown in the figure below:

The screenshot displays the 'AUDIT ADMINISTRATOR' interface. At the top, there are navigation tabs for 'Home' and 'Log'. Below these are input fields for 'log generation start time' and 'log generation end time', along with a 'query' button. An 'Operate object' dropdown menu is set to 'Current selected data', with an 'export' button next to it. The main area is a table with the following data:

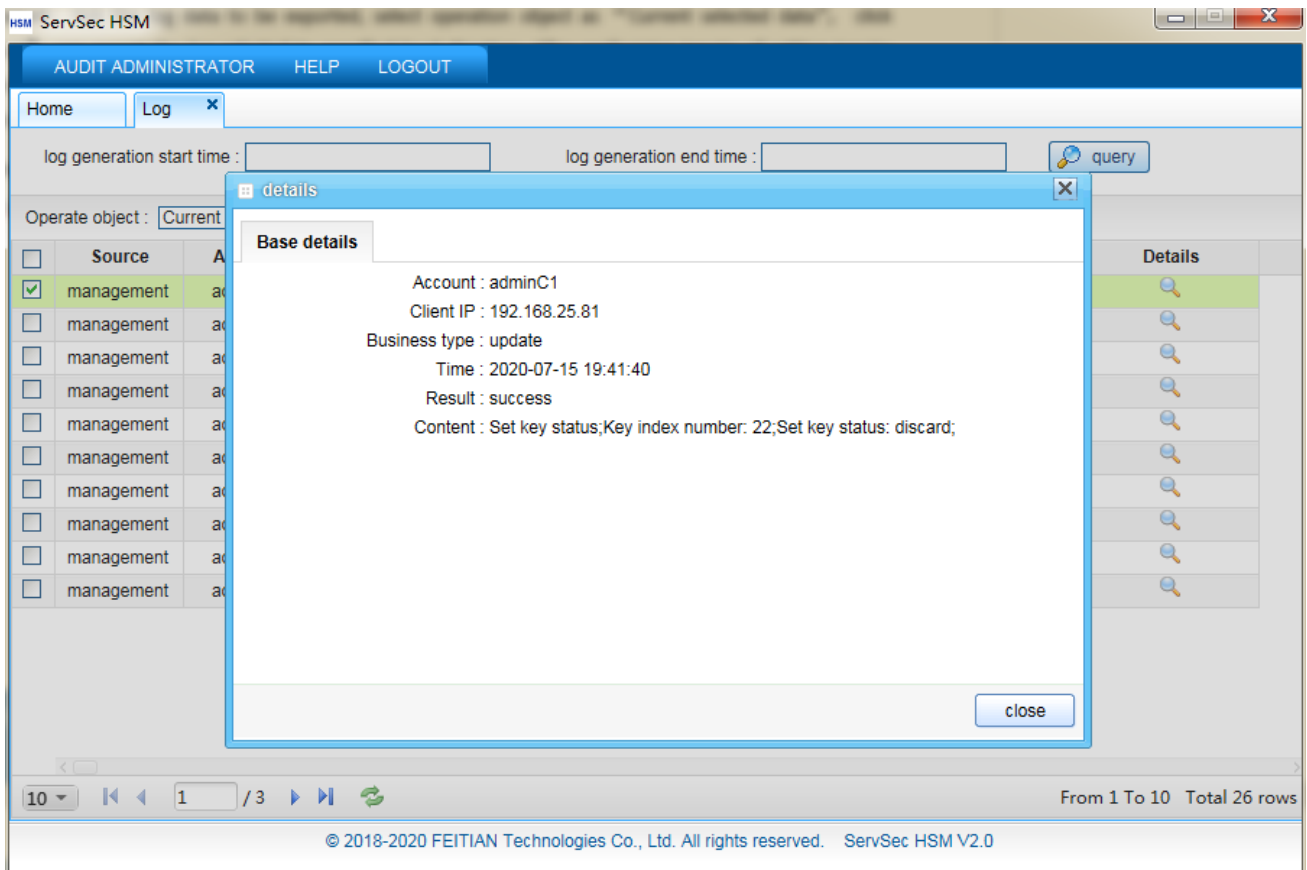
<input type="checkbox"/>	Source	Account	Client IP	Business type	Result	Time	Content	Details
<input type="checkbox"/>	management	adminC1	192.168.25.81	update	success	2020-07-15 19:41:40	Set key status;Key index	
<input type="checkbox"/>	management	adminC1	192.168.25.81	add	success	2020-07-15 19:41:36	Add key;Key index number:	
<input type="checkbox"/>	management	adminC1	192.168.25.81	add	success	2020-07-15 19:40:28	Add key;Key index number:	
<input type="checkbox"/>	management	adminC1	192.168.25.81	update	success	2020-07-15 19:35:45	Set key status;Key index	
<input type="checkbox"/>	management	adminC1	192.168.25.81	download	success	2020-07-15 19:34:23	Back up keys;	
<input type="checkbox"/>	management	adminB1	192.168.25.81	delete	success	2020-07-15 19:20:20	Delete operator [test];	
<input type="checkbox"/>	management	adminC1	192.168.25.81	update	success	2020-07-15 17:38:32	Set key status;Key index	
<input type="checkbox"/>	management	adminC1	192.168.25.81	update	success	2020-07-15 17:37:26	Set key status;Key index	
<input type="checkbox"/>	management	adminC1	192.168.25.81	download	success	2020-07-15 17:31:35	Back up keys;	
<input type="checkbox"/>	management	adminC1	192.168.25.81	update	success	2020-07-15 16:01:32	Set key status;Key index	

At the bottom of the table, there is a pagination bar showing '10' items per page, '1 / 3' pages, and 'From 1 To 10 Total 26 rows'. The footer contains the text: '© 2018-2020 FEITIAN Technologies Co., Ltd. All rights reserved. ServSec HSM V2.0'.

Inquiry: operator can perform log inquiry by selecting start/end time.

Export: tick the log data to be exported, select operation object as “Current selected data”, and click **【export】** to export the log selected to specified local directory. After performing inquiry of setting inquiry conditions, select operation object as “Current query data” and click **【export】** to export the log inquired to specified local directory.

Detail information: click **【Details】** in operating column of specified log data. A detailed info box will appear. Operator can check this log info, as shown in the figure below:



4.4.3.2 Operator log

This function block supports inquiry, checking, export functions on operator log files; operator can inquire and export corresponding operator log by the starting/ending time of log generation. Click **【Operator log】** in menu list of Audit Manager to enter operator log page, as shown in the figure below:

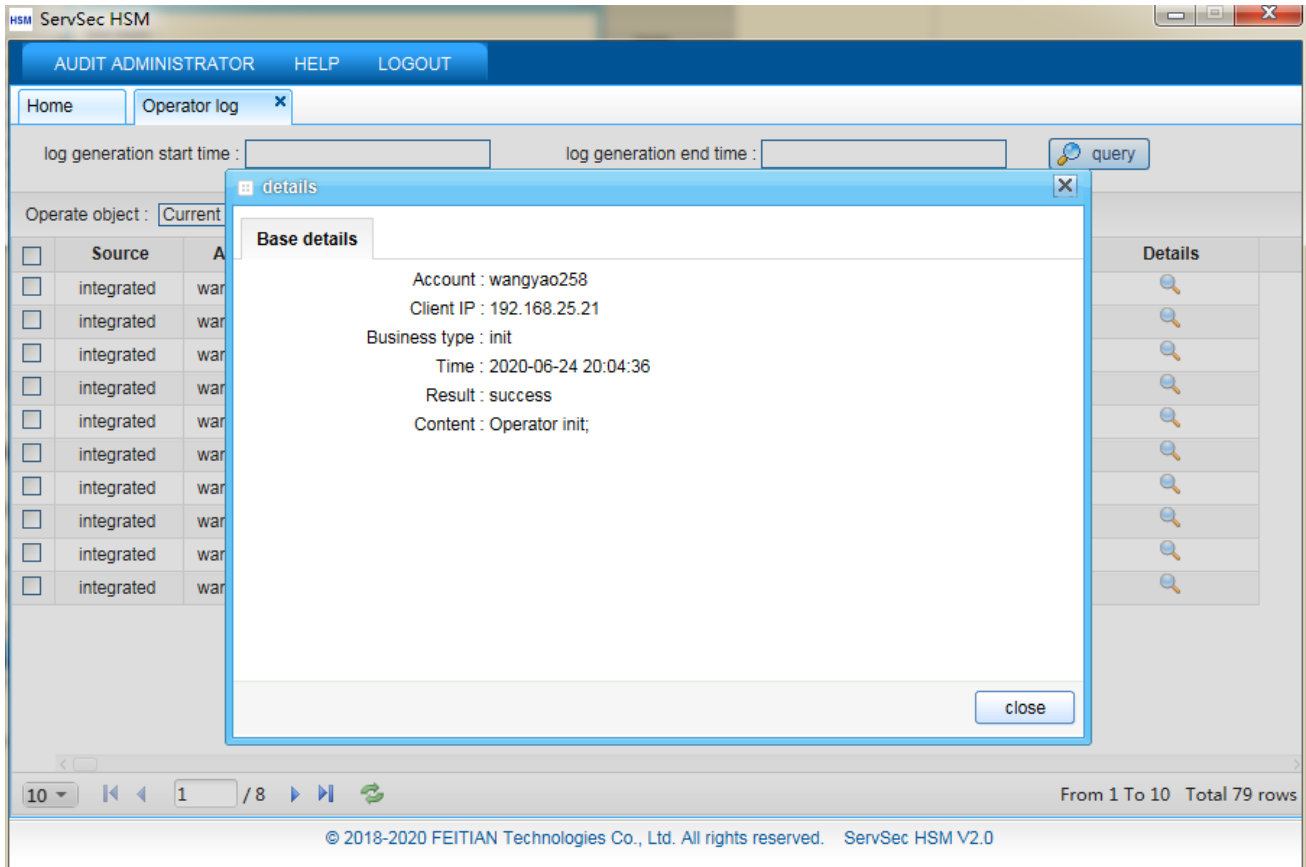
The screenshot displays the 'AUDIT ADMINISTRATOR' interface for 'ServSec HSM'. It features a navigation bar with 'HOME', 'OPERATOR LOG', and 'LOGOUT' options. Below the navigation bar, there are input fields for 'log generation start time' and 'log generation end time', along with a 'query' button. The main area contains a table with columns for 'Source', 'Account', 'Client IP', 'Business type', 'Result', 'Time', 'Content', and 'Details'. The table lists ten log entries, all with a status of 'success' and content 'Operator init;'. At the bottom, there is a pagination control showing '1 / 8' and 'From 1 To 10 Total 79 rows'. The footer includes the copyright notice: '© 2018-2020 FEITIAN Technologies Co., Ltd. All rights reserved. ServSec HSM V2.0'.

<input type="checkbox"/>	Source	Account	Client IP	Business type	Result	Time	Content	Details
<input type="checkbox"/>	integrated	wangyao258	192.168.25.21	init	success	2020-06-24 20:04:36	Operator init;	
<input type="checkbox"/>	integrated	wangyao258	192.168.25.21	init	success	2020-06-24 20:04:35	Operator init;	
<input type="checkbox"/>	integrated	wangyao258	192.168.25.21	init	success	2020-06-24 20:04:35	Operator init;	
<input type="checkbox"/>	integrated	wangyao258	192.168.25.21	init	success	2020-06-24 20:04:35	Operator init;	
<input type="checkbox"/>	integrated	wangyao258	192.168.25.21	init	success	2020-06-24 20:04:35	Operator init;	
<input type="checkbox"/>	integrated	wangyao258	192.168.25.21	init	success	2020-06-24 18:34:20	Operator init;	
<input type="checkbox"/>	integrated	wangyao258	192.168.25.21	init	success	2020-06-24 18:34:20	Operator init;	
<input type="checkbox"/>	integrated	wangyao258	192.168.25.21	init	success	2020-06-24 18:34:20	Operator init;	
<input type="checkbox"/>	integrated	wangyao258	192.168.25.21	init	success	2020-06-24 18:34:20	Operator init;	

Inquiry: can perform log inquiry by selecting starting/ending time.

Export: tick the log data to be exported, select operating object as “Current selected data” and click **【export】**. The selected log data will be exported to a specified local directory. Set inquiry conditions and check; select operating object as “Current query data” and click **【export】** to export the log inquired to a specified local directory.

Detail information: click **【Details】** in operating column of specified log data. A detailed info box will appear. Operator can check that log data record.



4.4.3.3 Configuring Running Log Parameters

This function can set size and retaining period of audit log.

Click **【Configure running log parameters】** in Audit Manager menu list, input parameters to be modified, click **【ok】**, setting success. Log will be stored follow this setting. The setting page is shown in the figure below:

HSM ServSec HSM

AUDIT ADMINISTRATOR HELP LOGOUT

Home Configure running log parameters

Log level : ERROR

Please input modified log retain days (calculated forward from current time, 1~365, unit: day) : 30

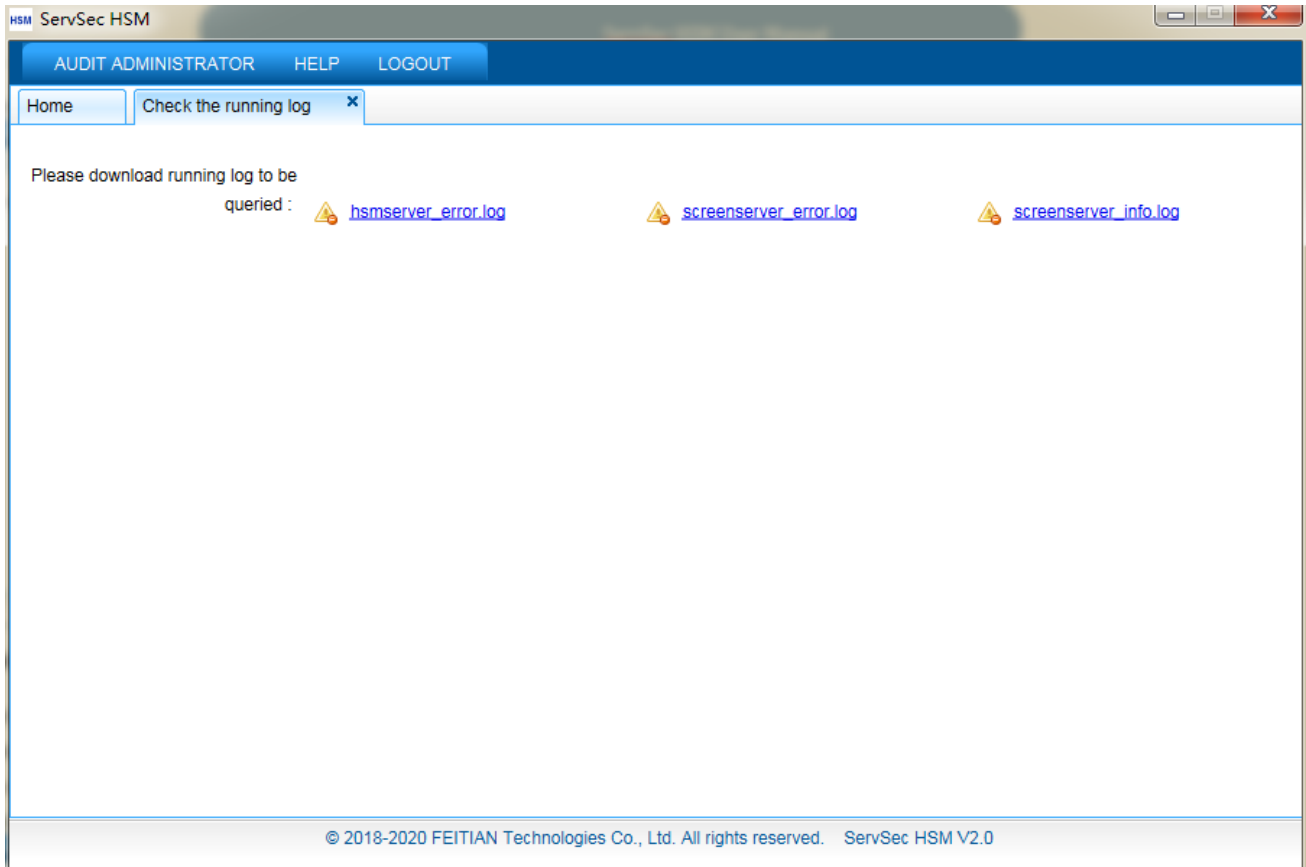
Please input log backup size critical value (unit: MB) : 10

save

© 2018-2020 FEITIAN Technologies Co., Ltd. All rights reserved. ServSec HSM V2.0

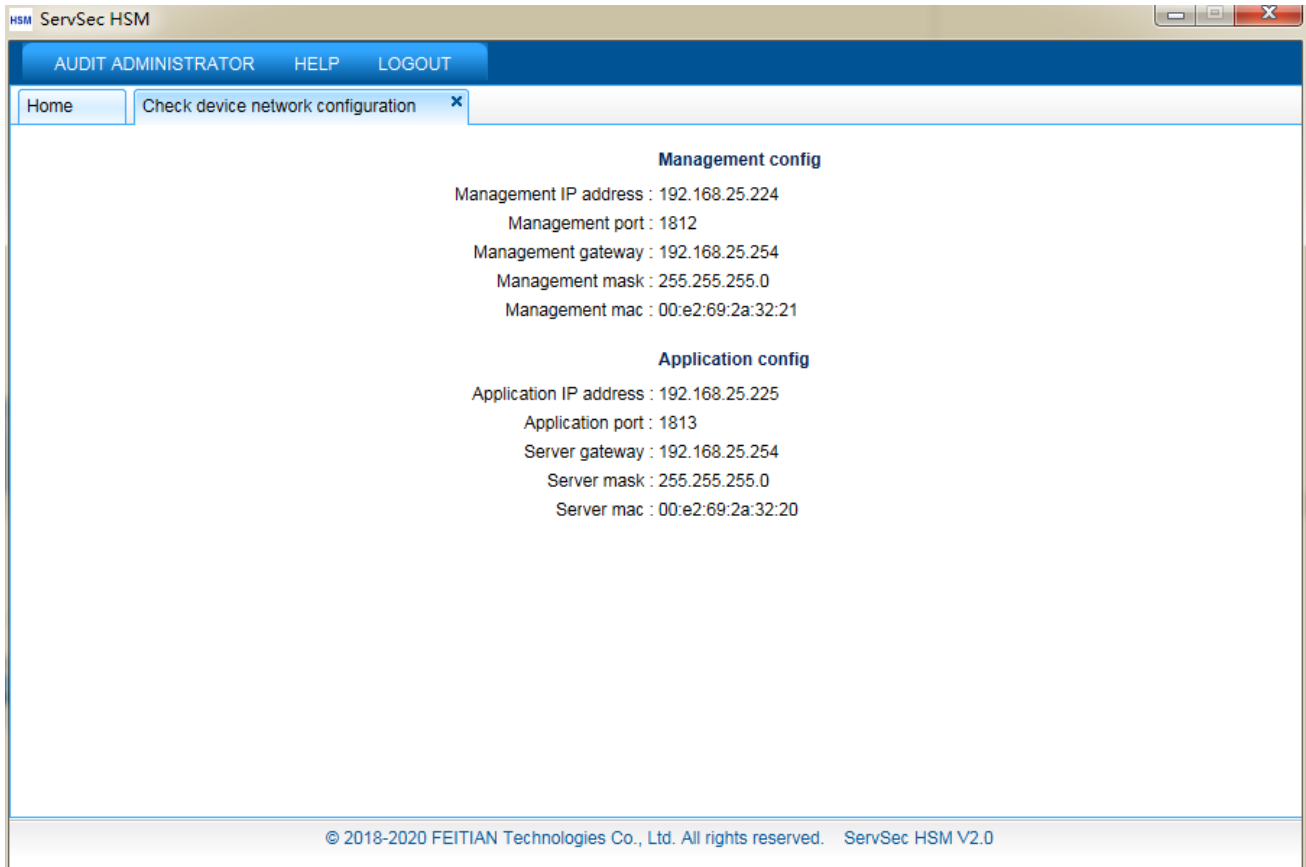
4.4.3.4 Check the running log

This module can view the running logs of all the managers and operators during operation, and supports downloading logs. You can download the logs to the local and provide them to the supplier for viewing. Click **【Check the running log】** in the Audit Manager menu list, as shown below:



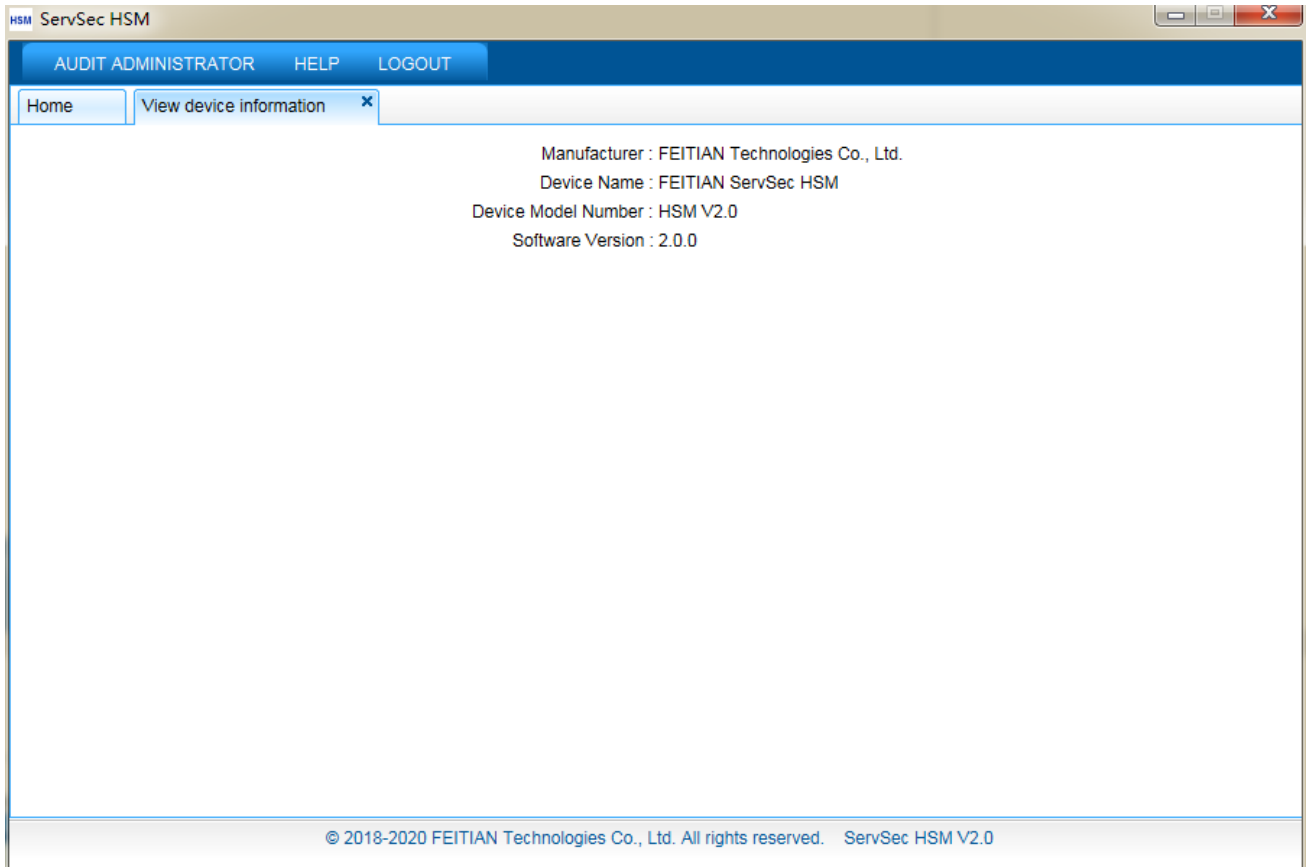
4.4.3.5 Check device network configuration

This function block supports checking management tool configuration and application configuration of current device. Click **【Check device network configuration】** in Audit Manager menu list, show network configuration of current device, as shown in the figure below:



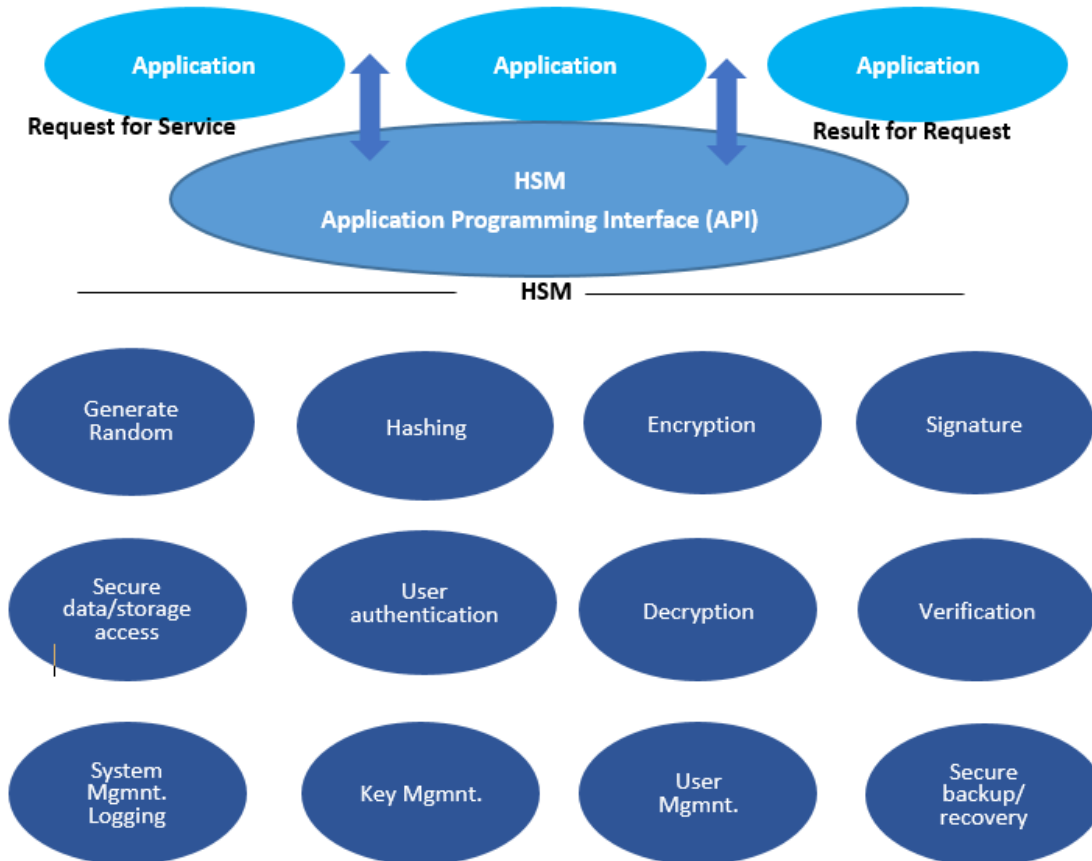
4.4.3.6 View Device Information

This function block supports device info checking function, click **【View device information】** in Audit Manager menu list, show current device info, including manufacturer, product name, model, etc, as shown in the figure below:



5 Application System Connection

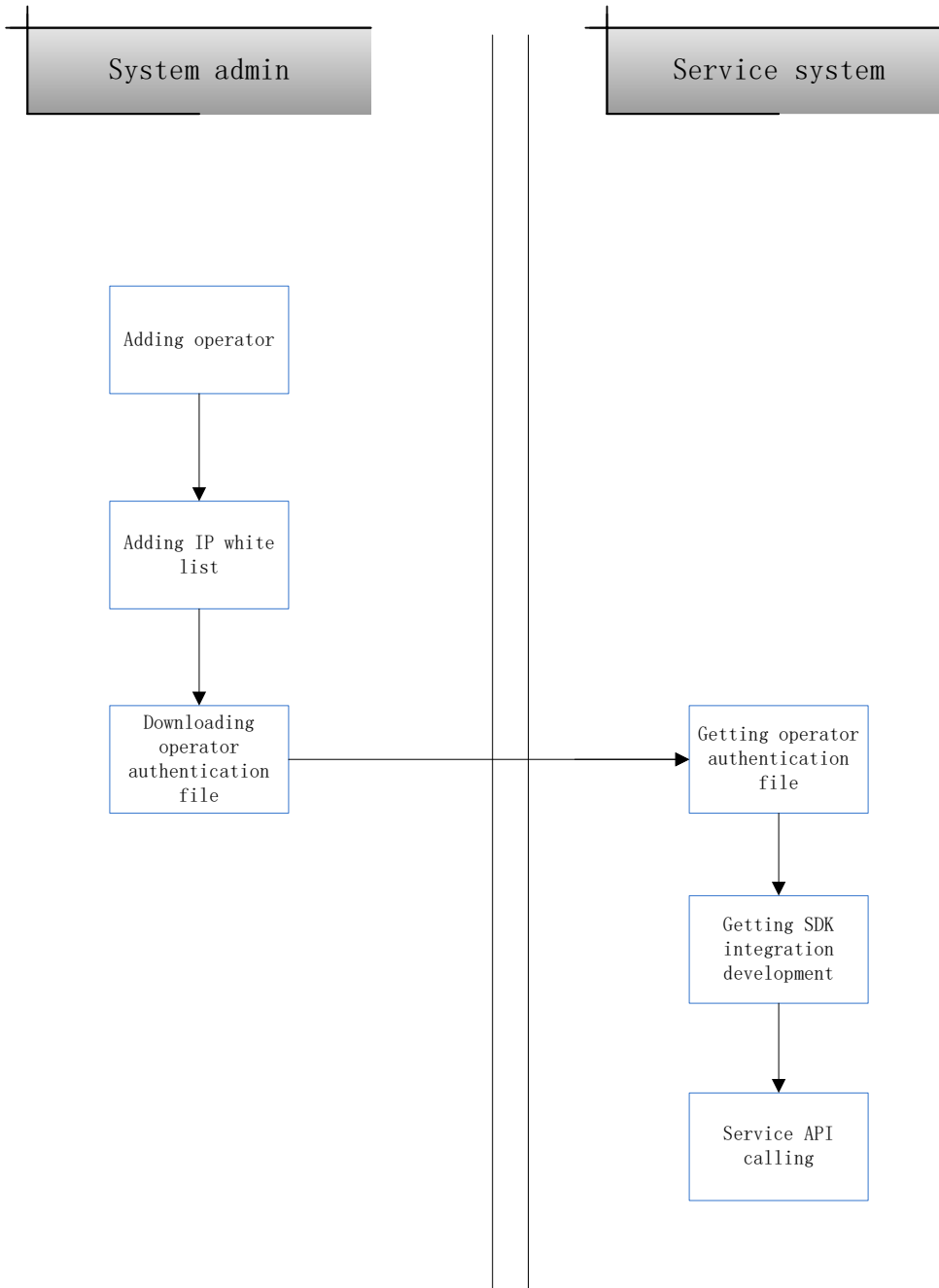
5.1 API Model



Application system communicates with HSM service by calling service API provided by HSM Cryptographic Module. For details regarding the description of HSM service APIs, please refer to product application integration development guidance.

5.2 Integration Process

The application system integrating HSM service process is shown in the figure below:

**Note: :**

- 1) System Manager needs to log on to management tool, add operator, download operator authentication file and send this file to integration developer of service system; add it into IP white list; only after the IP of the service system client to be connected to the service has been added to the white list can the service system client can visit the service normally.
- 2) Service system (that is the operator) integration developer gets authentication file and SDK and performs integration development according to integration development guidance. Once complete, operator can call services according to business demand.

6 Note

In the case of self-test failure, the touch screen will show the cause of the failure and the buzzer will sound regularly. The following is the list of causes for failure and the corresponding buzzer sound:

Self-test failure reason	Buzzer sounds
Forced demolitions	2 long & 1 short
The hard disk is replaced	2 long & 2 short
Memory is replaced	2 long & 3 short
The card-reader is replaced	2 long & 4 short
The network-card is replaced	3 long & 1 short
Network-card is not available	3 long & 2 short
Arithmetic-chip is replaced	3 long and 3 short
Software tampered	3 long and 4 short
Other reasons	4 long and 4 short
Database initialization failed	a long beep, 10 seconds