翼安服务器密码机
用户手册

山东华翼微电子技术股份有限公司

版本更新记录表			
序号	版本号	版本更改说明	更改日期
1	V1.0	首次发布	
2			
3			
4			
5			
6			
7			
8			
9			
10			

声 明

版权声明

特别提示

我们做了大量的努力使本文档尽可能的完备和准确，但疏漏和缺陷之处在所难免。任何人或实体由于本文档提供的信息造成的任何损失或损害，山东华翼微电子技术股份有限公司不承担任何义务或责任。

山东华翼微电子技术股份有限公司保留未经通知用户对本文档内容进行修改的权利。

联系我们

如果您对本文档有任何疑问、意见或建议，请与我们联系。对您的帮助，我们十分感激。

公司电话：0531-66680161

公司邮箱：shandonghuayi@holichip.com

公司地址：山东济南高新区舜泰北路933号19层

目 录

1 产品概述

1.1 产品简介

翼安服务器密码机是由山东华翼微电子技术股份有限公司自主研发的高性能密码设备，产品严格遵循国家相关产品技术规范进行设计，内置经国家密码管理局审批的高速密码模块，支持国家密码管理局认可的密码算法，适用于各类密码安全应用系统进行高速的、多任务并行处理的密码运算。可以满足应用系统数据的加密解密、签名/验证的要求，实现应用的数据的机密性和完整性保护，同时可提供安全、完善的密钥管理机制。

应用系统通过调用服务器密码机提供的API接口来使用密码服务，密码机API与密码机之间的调用过程对上层应用透明，应用开发商能够快速的使用密码机所提供的安全功能。密码机API接口符合密码产品标准接口规范，通用性好，能够满足大多数应用系统的要求，在应用系统安全方面具有广泛的应用前景。

2 产品操作说明

2.1 初次使用服务器密码机流程

首先，通过IE10（其他浏览器可以根据浏览器提示进行）浏览器登录服务器密码机IP（eth0默认是192.168.18.239）：https://192.168.18.239，弹出如图1界面：

图 2

单击“继续浏览此网站（不推荐）”，进入用户登录界面如图2

图 2

当初次登陆加密机时，没有任何管理员的添加，所以默认用户名：admin，密码：admin，点击登录，可以进入配置页面。可以正常通过浏览器访问服务器密码机进行相关配置操作。使用服务器密码机时需要从web页面首页下载客户端软件。首先点击客户端下载，下载“客户端”软件setup.exe。

安装setup.exe控件，以便支持用户管理。操作步骤如下：

以管理员身份运行setup.exe，选择“下一步”：

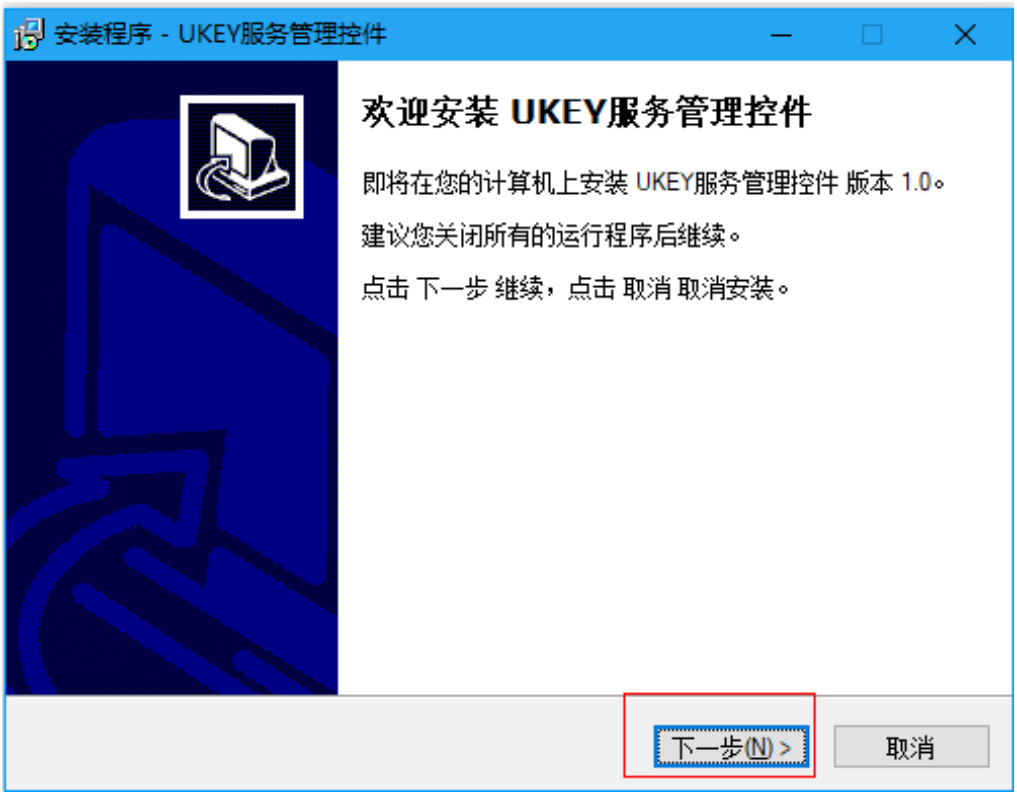

图 3

继续，下一步；

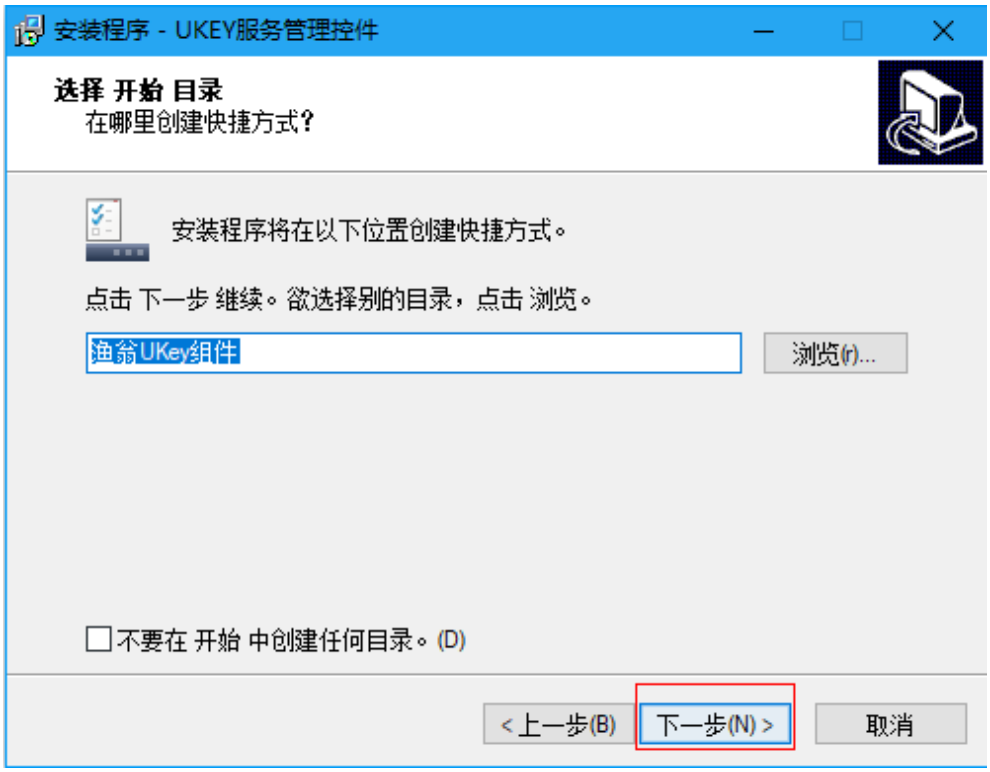
安装程序 - UKEY服务管理控件
选择 开始 目录
在哪里创建快捷方式?
安装程序将在以下位置创建快捷方式。
点击 下一步 继续。欲选择别的目录，点击 浏览。
渔翁UKey组件
浏览(r)...
不要在 开始 中创建任何目录。(D)
< 上一步(B)
下一步(N) >
取消

图 4

继续，下一步；

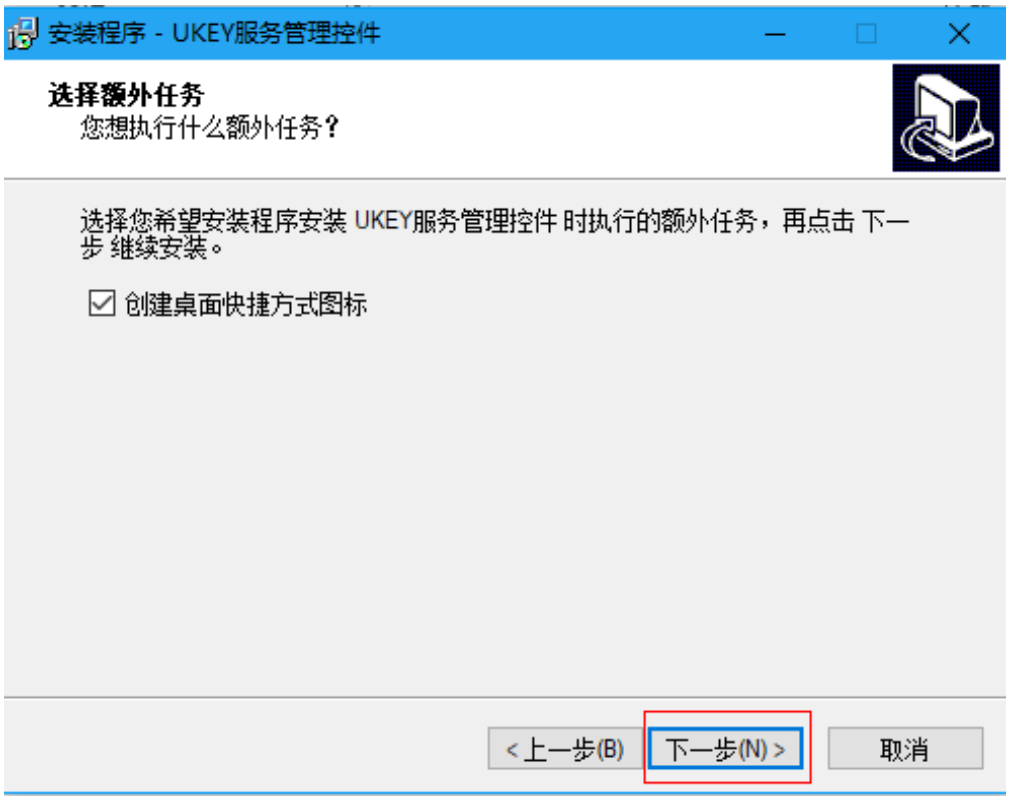
安装程序 - UKEY服务管理控件
选择额外任务
您想执行什么额外任务?
选择您希望安装程序安装 UKEY服务管理控件 时执行的额外任务，再点击 下一步 继续安装。
创建桌面快捷方式图标
< 上一步(B)
下一步(N) >
取消

图 5

继续，选择“安装”；

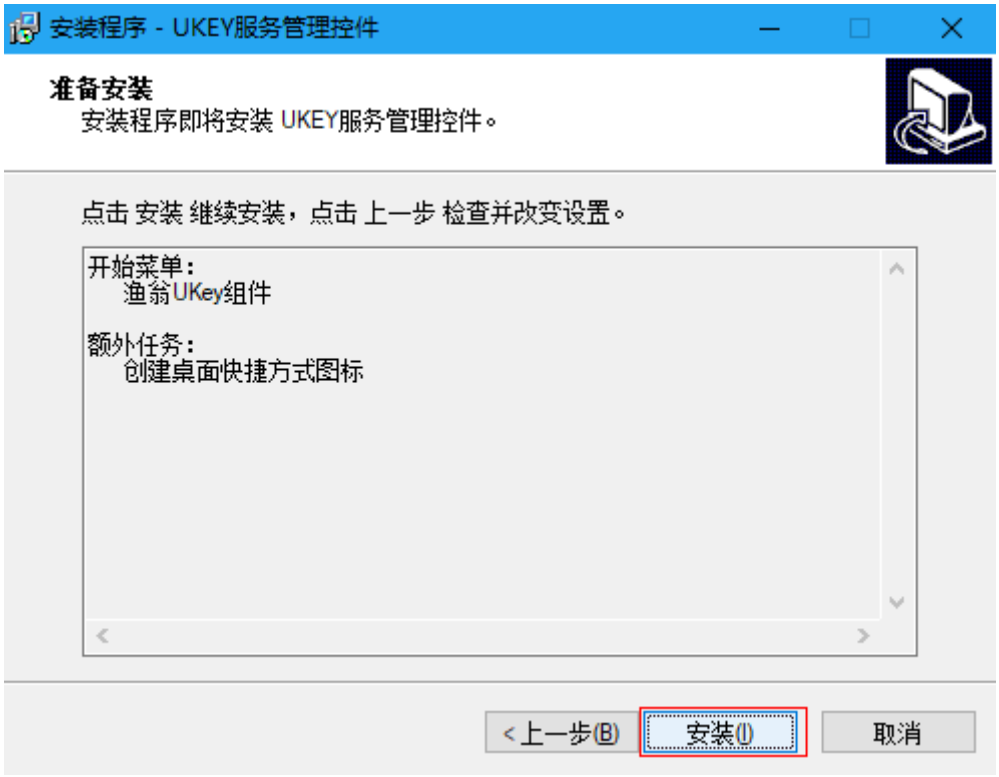

图 6

安装完成后，相关服务已经启动，后续可以进行用户管理等相关操作。

3 服务器密码机操作配置

3.1 服务器密码机服务配置

3.1.1 服务器密码机网络配置

对密码机的网络配置，需要满足管理员权限。初次登录，系统未添加管理员，登录后权限默认为管理员权限。

单击左侧菜单栏“服务配置”按钮，并单击“网络配置”按钮，如图 7

选择网卡端口，输入IP和掩码，网关没有可以不输。每个网口可单独设置服务类型：“配置管理”用于web管理；“主服务”用于主服务调用。“兼容”模式即网口可同时提供web管理和主服务调用。“聚合”模式需要先选择需要配置的网口，配置好IP选择聚合模式，单击修改，然后循环此操作，直到所有需要聚合的网口配置完成后，再重启

加密机。聚合模式为主备，端口号较小的为主口，IP以此端口为主。

IP配置完成后需要重启加密机后才能生效。点击设备管理菜单—>服务器重启，点击服务器重启会提示设备重启启动,请稍等。设备重启后,加密机IP会变为修改后的IP。

图 7

3.1.2 路由配置

对密码机的路由配置，需要满足管理员权限。

单击左侧菜单栏“服务配置”按钮，并单击“路由配置”按钮，如图8。

输入“目标网络”、“子网掩码”、“网关地址”，点击“新增”即可添加路由信息，并且立即生效。选中需要删除的路由信息，然后点击“删除”按钮，即可删除当前路由信息，并且立即生效。

图 8

3.1.3 Syslog配置

对密码机的syslog配置，需要满足管理员权限。

单击左侧菜单栏“服务配置”按钮，并单击“syslog配置”按钮，如图9。

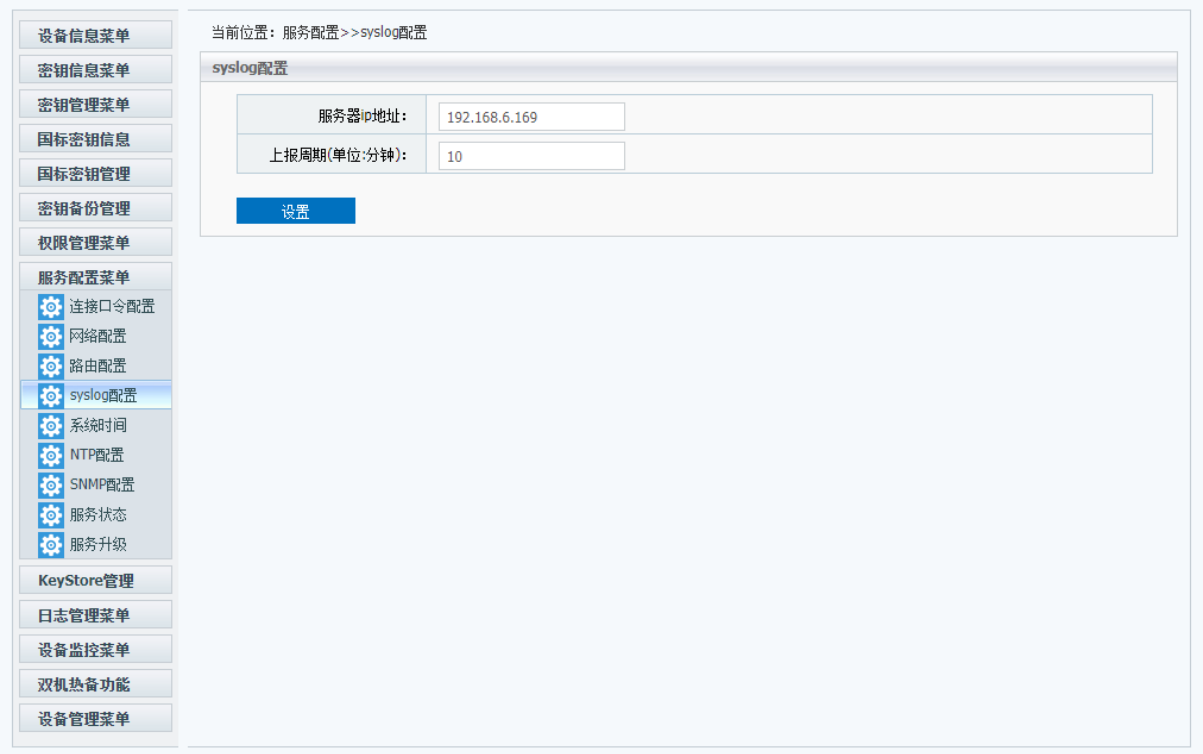

图 9

3.1.4 系统时间设置

对密码机的时间配置，需要满足管理员权限。

单击左侧菜单栏“服务配置”按钮，并单击“时间配置”按钮，如**错误!未找到引用源。**0。可查看和设置服务器的系统时间。

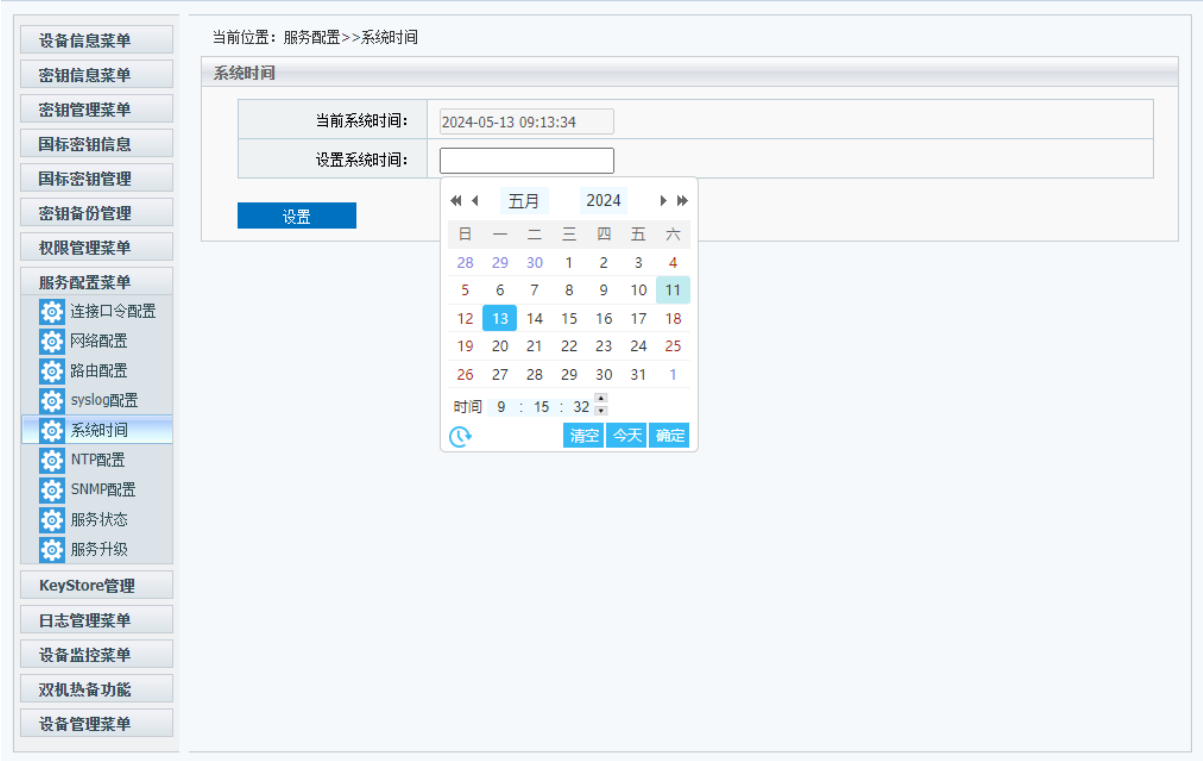

图 30

3.1.5 服务升级

对密码机的服务升级，需要满足管理员权限。

单击左侧菜单栏“服务配置”按钮，并单击“服务升级”按钮，如**错误!未找到引用源。**1。可进行服务器的本地升级，升级包需要由厂家提供。

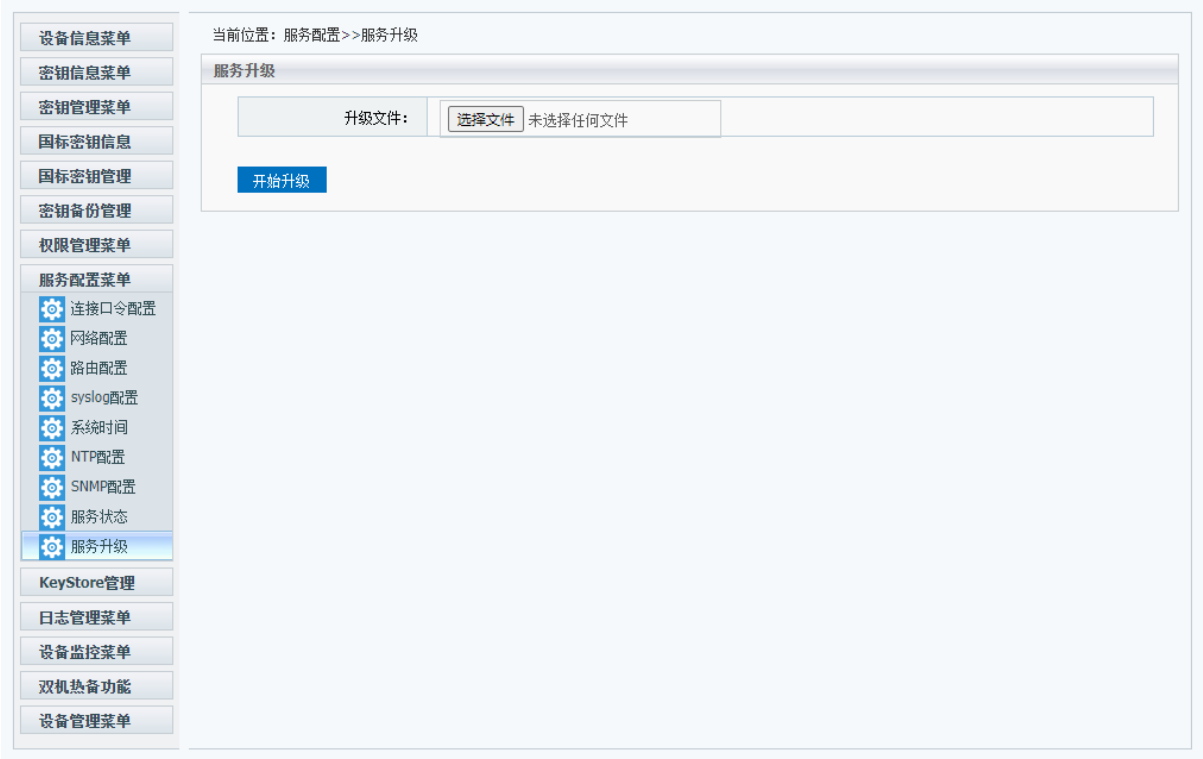

图 31

3.2 服务器密码机权限管理配置

3.2.1 管理员、审计员添加

单击左侧菜单栏“权限管理”按钮，在配置终端（指个人笔记本电脑，不是服务器密码机）USB口中插入key并单击“用户添加”按钮，如图12。

图 32

选择管理员角色，用户口令默认为12345678，点击“添加用户”按钮，成功后会在“用户管理”中显示已添加的管理员。输入口令后，再单击“登录”按钮，如图13。 添加用户必须满足管理员权限，即有半数以上的管理员登陆。

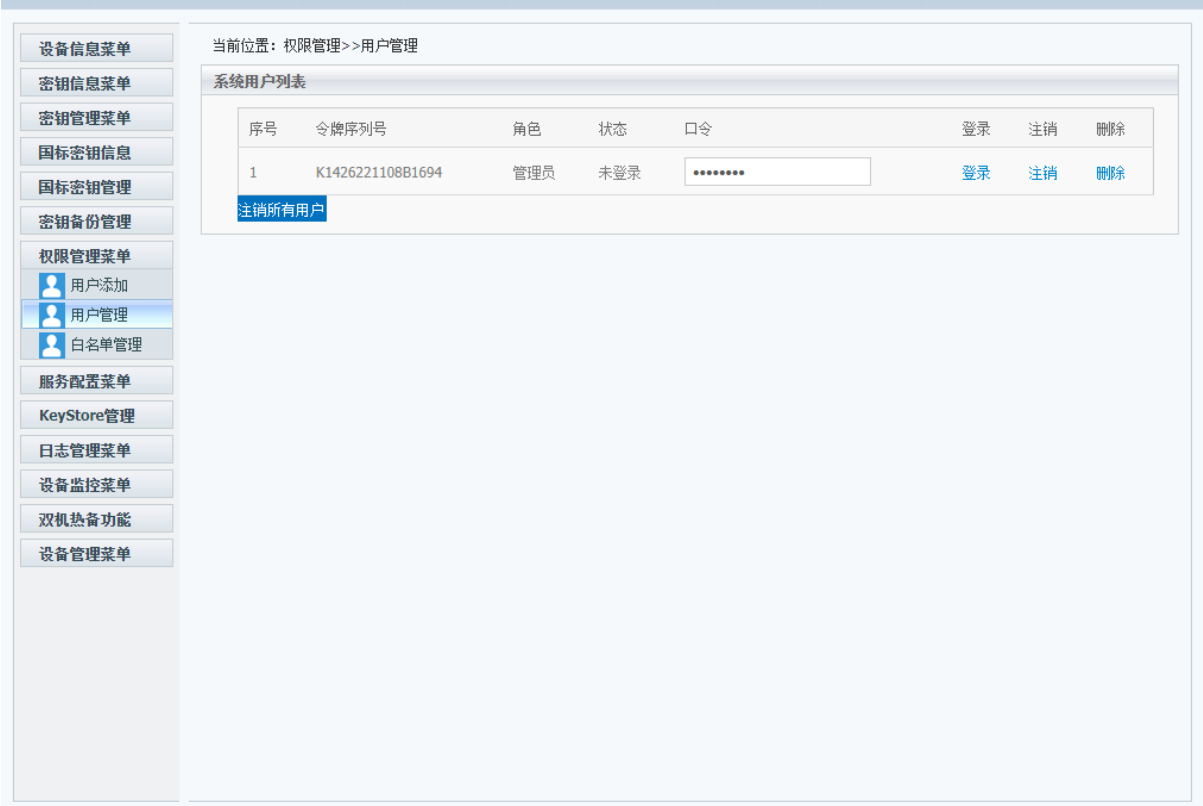

图 33

登录口令输入添加的管理员口令，默认是12345678。登录成功后会提示登录成功。同时会修改登录状态为“已登录”。

把添加管理员的key做上标记，然后拔掉key，重新插入下一个key进行管理员添加，步骤与第一个相同。

请依次使用如上方法添加五个管理员。

当有半数以上的管理员登陆时，即获得管理员权限，如果管理员状态显示“未登录”即使加密机内部含有半数以上的管理员，也不具有管理员权限。

添加完5个管理员后，单击左侧菜单栏添加用户，添加审计管理员。审计管理员的权限是可以查看审计日志，进行审计操作以及删除审计日志。添加审计管理员方法与添加管理员相同。

3.2.2 用户删除

删除用户必须满足管理员权限，即有半数以上的管理员登陆。

删除用户时，在要删除的用户右侧单击“删除”按钮。如图14。

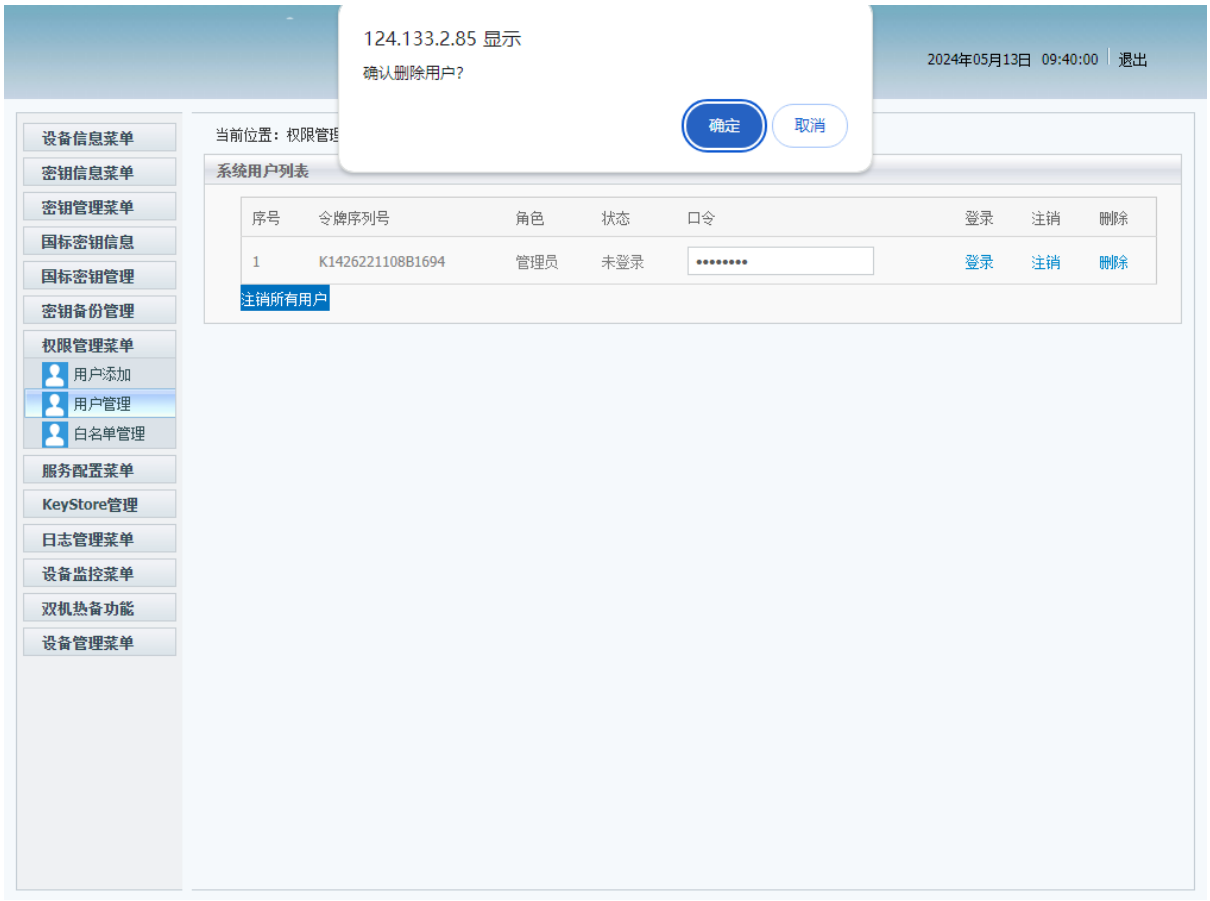

图 34

3.2.3 注销所有用户

在符合半数登陆的情况下，点击“注销所有用户”，会同时注销管理员和审计员，状态显示为“未登录”。如图15。

图 35

审计管理员注销后，将无法查看、审计、删除审计日志。如图16。

图 36

3.2.4 修改用户口令

单击“修改口令”按钮后，如图17。

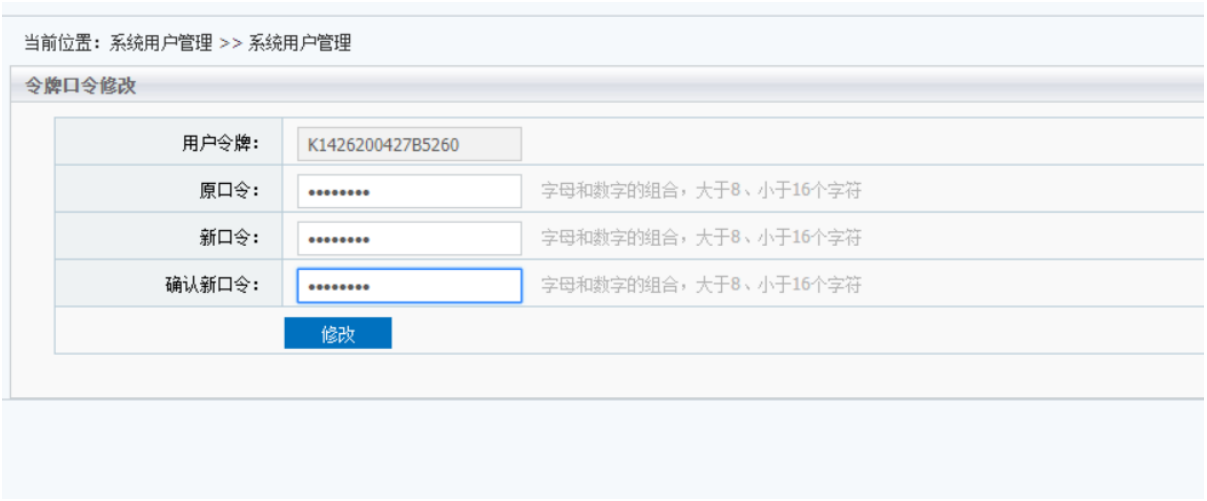

图 37

在旧口令中输入USB KEY原有口令，新口令框中输入新口令，确认口令框中再输一次新口令。单击“修改”按钮完成口令修改。

3.2.5 白名单配置

单击左侧菜单栏“权限管理”按钮，并单击“白名单管理”按钮，如图18。如果白名单内没有任何IP则允许所有IP访问服务器密码机。

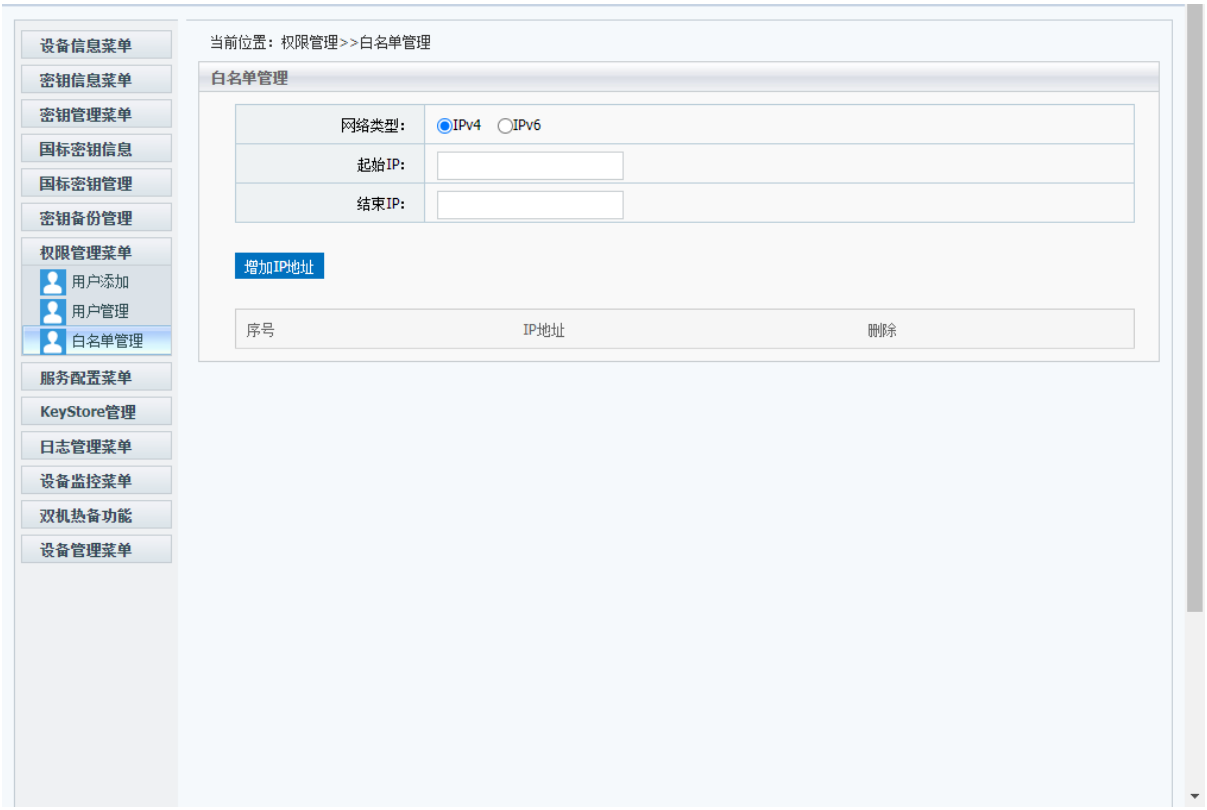

图 38

输入起始IP和结束IP，添加白名单成功后，只有白名单范围的ip地址，才允许访问加密机服务。如图19。

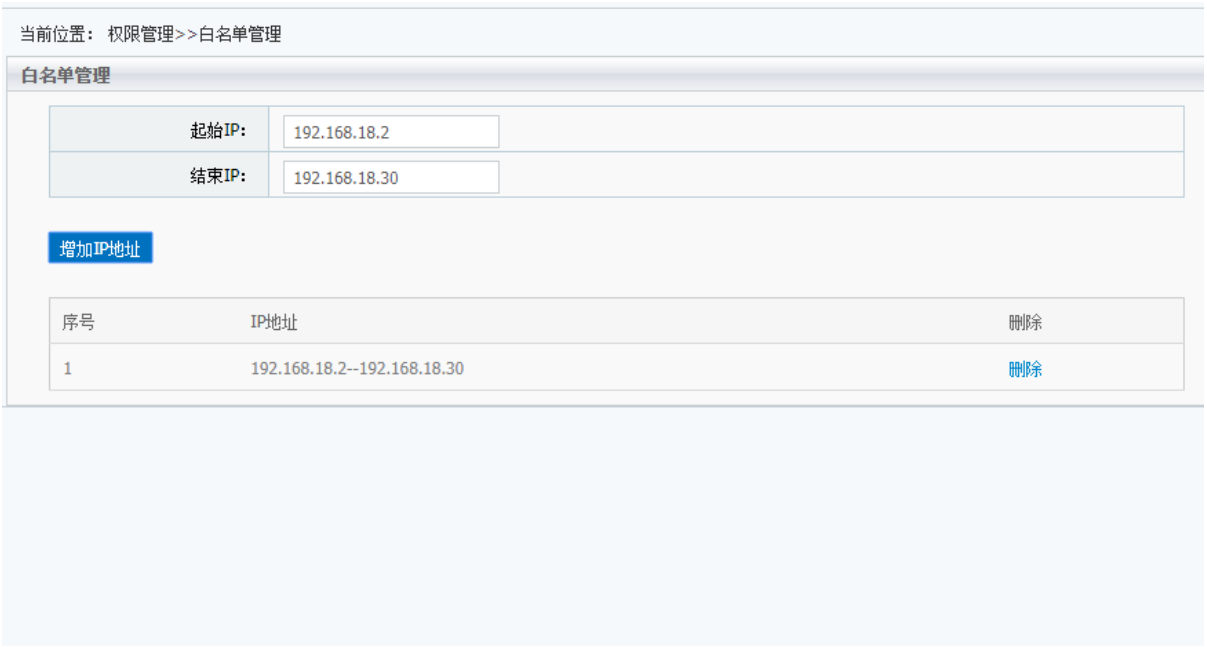

图 39

3.3 服务器密码机设备信息查看

单击左侧菜单栏“设备信息”按钮，进入设备信息查看页面，如图20。

图 20

单击左侧菜单栏“密钥信息”按钮，进入密钥信息查看页面，查看RSA密钥、SM2密钥、SM9主密钥、SM9用户密钥、对称密钥，如**错误!未找到引用源。**-28。其中，如果加密机支持SM9密钥，则SM9相关密钥信息页正常显示，如果不支持，则不显示。

当前位置：密钥信息 >>RSA密钥信息

RSA密钥信息

0:[****]	1:[1024]	2:[2048]	3:[1024]	4:[1024]	5:[1024]	6:[1024]	7:[1024]	8:[1024]	9:[1024]
10:[1024]	11:[1024]	12:[1024]	13:[1024]	14:[1024]	15:[1024]	16:[1024]	17:[1024]	18:[1024]	19:[1024]
20:[1024]	21:[1024]	22:[1024]	23:[1024]	24:[1024]	25:[1024]	26:[1024]	27:[1024]	28:[1024]	29:[1024]
30:[1024]	31:[1024]	32:[1024]	33:[1024]	34:[1024]	35:[1024]	36:[1024]	37:[1024]	38:[1024]	39:[1024]
40:[1024]	41:[1024]	42:[1024]	43:[1024]	44:[1024]	45:[1024]	46:[1024]	47:[1024]	48:[1024]	49:[1024]
50:[1024]	51:[1024]	52:[1024]	53:[1024]	54:[1024]	55:[1024]	56:[1024]	57:[1024]	58:[1024]	59:[1024]
60:[1024]	61:[1024]	62:[1024]	63:[1024]	64:[1024]	65:[1024]	66:[1024]	67:[1024]	68:[1024]	69:[1024]
70:[1024]	71:[1024]	72:[1024]	73:[1024]	74:[1024]	75:[1024]	76:[1024]	77:[1024]	78:[1024]	79:[1024]
80:[1024]	81:[1024]	82:[1024]	83:[1024]	84:[1024]	85:[1024]	86:[1024]	87:[1024]	88:[1024]	89:[1024]
90:[1024]	91:[1024]	92:[1024]	93:[1024]	94:[1024]	95:[1024]	96:[1024]	97:[1024]	98:[1024]	99:[1024]
100:[1024]	101:[****]	102:[****]	103:[****]	104:[****]	105:[****]	106:[****]	107:[****]	108:[****]	109:[****]
110:[****]	111:[****]	112:[****]	113:[****]	114:[****]	115:[****]	116:[****]	117:[****]	118:[****]	119:[****]
120:[****]	121:[****]	122:[****]	123:[****]	124:[****]	125:[****]	126:[****]	127:[****]	128:[****]	129:[****]
130:[****]	131:[****]	132:[****]	133:[****]	134:[****]	135:[****]	136:[****]	137:[****]	138:[****]	139:[****]

图 21

当前位置：密钥信息>>SM2密钥信息

SM2密钥

0:[***]	1:[256]	2:[256]	3:[256]	4:[256]	5:[256]	6:[256]	7:[256]	8:[256]	9:[256]
10:[256]	11:[256]	12:[256]	13:[256]	14:[256]	15:[256]	16:[256]	17:[256]	18:[256]	19:[256]
20:[256]	21:[256]	22:[256]	23:[256]	24:[256]	25:[256]	26:[256]	27:[256]	28:[256]	29:[256]
30:[256]	31:[256]	32:[256]	33:[256]	34:[256]	35:[256]	36:[256]	37:[256]	38:[256]	39:[256]
40:[256]	41:[256]	42:[256]	43:[256]	44:[256]	45:[256]	46:[256]	47:[256]	48:[256]	49:[256]
50:[256]	51:[256]	52:[256]	53:[256]	54:[256]	55:[256]	56:[256]	57:[256]	58:[256]	59:[256]
60:[256]	61:[256]	62:[256]	63:[256]	64:[256]	65:[256]	66:[256]	67:[256]	68:[256]	69:[256]
70:[256]	71:[256]	72:[256]	73:[256]	74:[256]	75:[256]	76:[256]	77:[256]	78:[256]	79:[256]
80:[256]	81:[256]	82:[256]	83:[256]	84:[256]	85:[256]	86:[256]	87:[256]	88:[256]	89:[256]
90:[256]	91:[256]	92:[256]	93:[256]	94:[256]	95:[256]	96:[256]	97:[256]	98:[256]	99:[256]
100:[256]	101:[***]	102:[***]	103:[***]	104:[***]	105:[***]	106:[***]	107:[***]	108:[***]	109:[***]
110:[***]	111:[***]	112:[***]	113:[***]	114:[***]	115:[***]	116:[***]	117:[***]	118:[***]	119:[***]
120:[***]	121:[***]	122:[***]	123:[***]	124:[***]	125:[***]	126:[***]	127:[***]	128:[***]	129:[***]
130:[***]	131:[***]	132:[***]	133:[***]	134:[***]	135:[***]	136:[***]	137:[***]	138:[***]	139:[***]

图 22

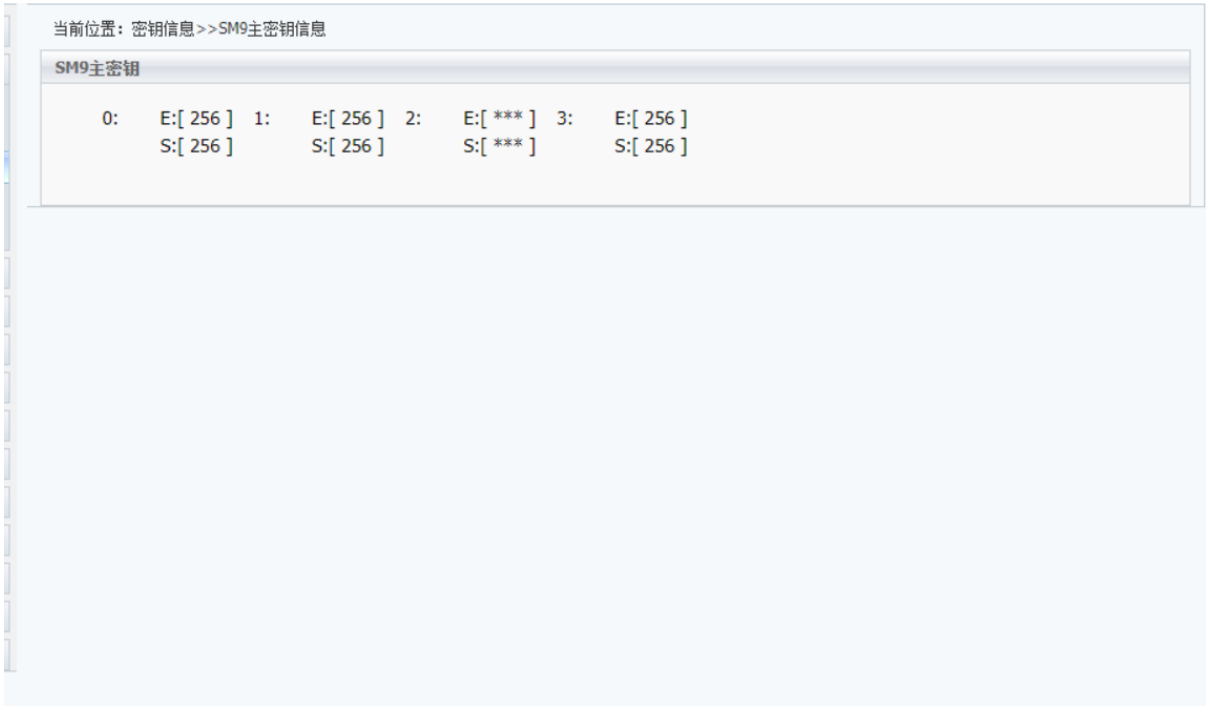
当前位置：密钥信息>>SM9主密钥信息
SM9主密钥
0: E:[256] S:[256]
1: E:[256] S:[256]
2: E:[***] S:[***]
3: E:[256] S:[256]

图 23

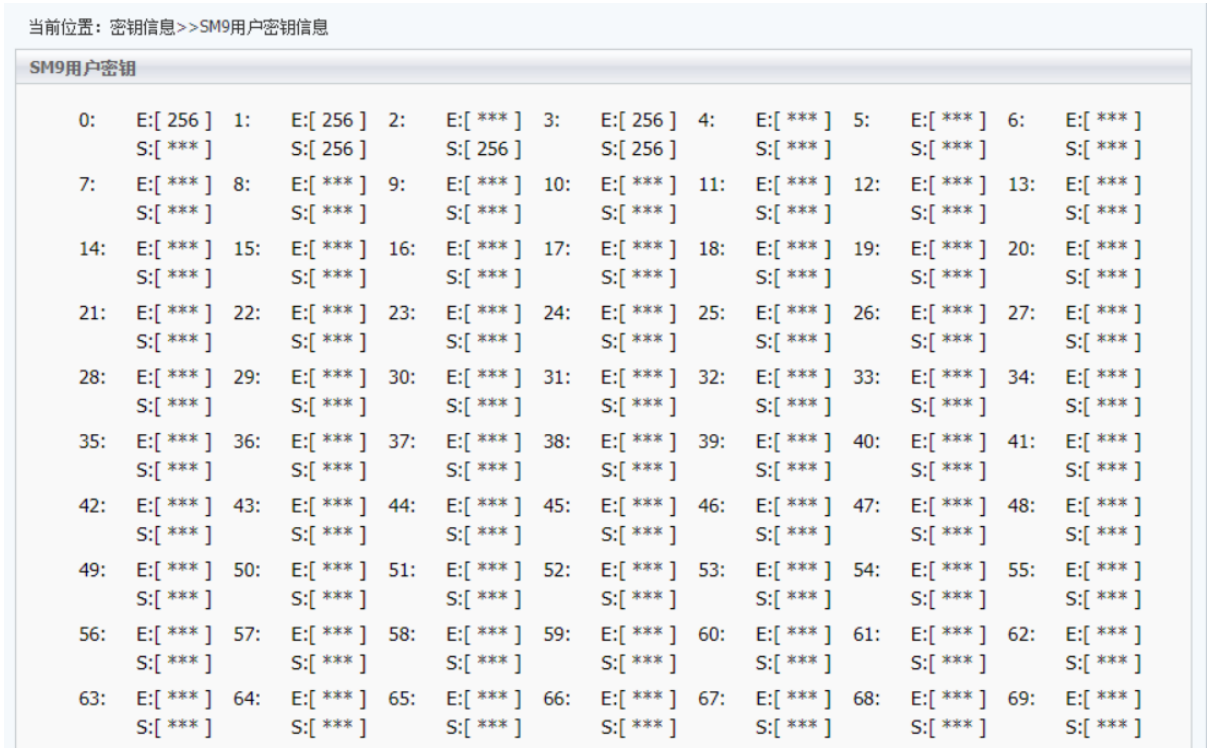
当前位置：密钥信息>>SM9用户密钥信息
SM9用户密钥
0: E:[256] S:[***]
1: E:[256] S:[256]
2: E:[***] S:[256]
3: E:[256] S:[256]
4: E:[***] S:[***]
5: E:[***] S:[***]
6: E:[***] S:[***]
7: E:[***] S:[***]
8: E:[***] S:[***]
9: E:[***] S:[***]
10: E:[***] S:[***]
11: E:[***] S:[***]
12: E:[***] S:[***]
13: E:[***] S:[***]
14: E:[***] S:[***]
15: E:[***] S:[***]
16: E:[***] S:[***]
17: E:[***] S:[***]
18: E:[***] S:[***]
19: E:[***] S:[***]
20: E:[***] S:[***]
21: E:[***] S:[***]
22: E:[***] S:[***]
23: E:[***] S:[***]
24: E:[***] S:[***]
25: E:[***] S:[***]
26: E:[***] S:[***]
27: E:[***] S:[***]
28: E:[***] S:[***]
29: E:[***] S:[***]
30: E:[***] S:[***]
31: E:[***] S:[***]
32: E:[***] S:[***]
33: E:[***] S:[***]
34: E:[***] S:[***]
35: E:[***] S:[***]
36: E:[***] S:[***]
37: E:[***] S:[***]
38: E:[***] S:[***]
39: E:[***] S:[***]
40: E:[***] S:[***]
41: E:[***] S:[***]
42: E:[***] S:[***]
43: E:[***] S:[***]
44: E:[***] S:[***]
45: E:[***] S:[***]
46: E:[***] S:[***]
47: E:[***] S:[***]
48: E:[***] S:[***]
49: E:[***] S:[***]
50: E:[***] S:[***]
51: E:[***] S:[***]
52: E:[***] S:[***]
53: E:[***] S:[***]
54: E:[***] S:[***]
55: E:[***] S:[***]
56: E:[***] S:[***]
57: E:[***] S:[***]
58: E:[***] S:[***]
59: E:[***] S:[***]
60: E:[***] S:[***]
61: E:[***] S:[***]
62: E:[***] S:[***]
63: E:[***] S:[***]
64: E:[***] S:[***]
65: E:[***] S:[***]
66: E:[***] S:[***]
67: E:[***] S:[***]
68: E:[***] S:[***]
69: E:[***] S:[***]

图 24

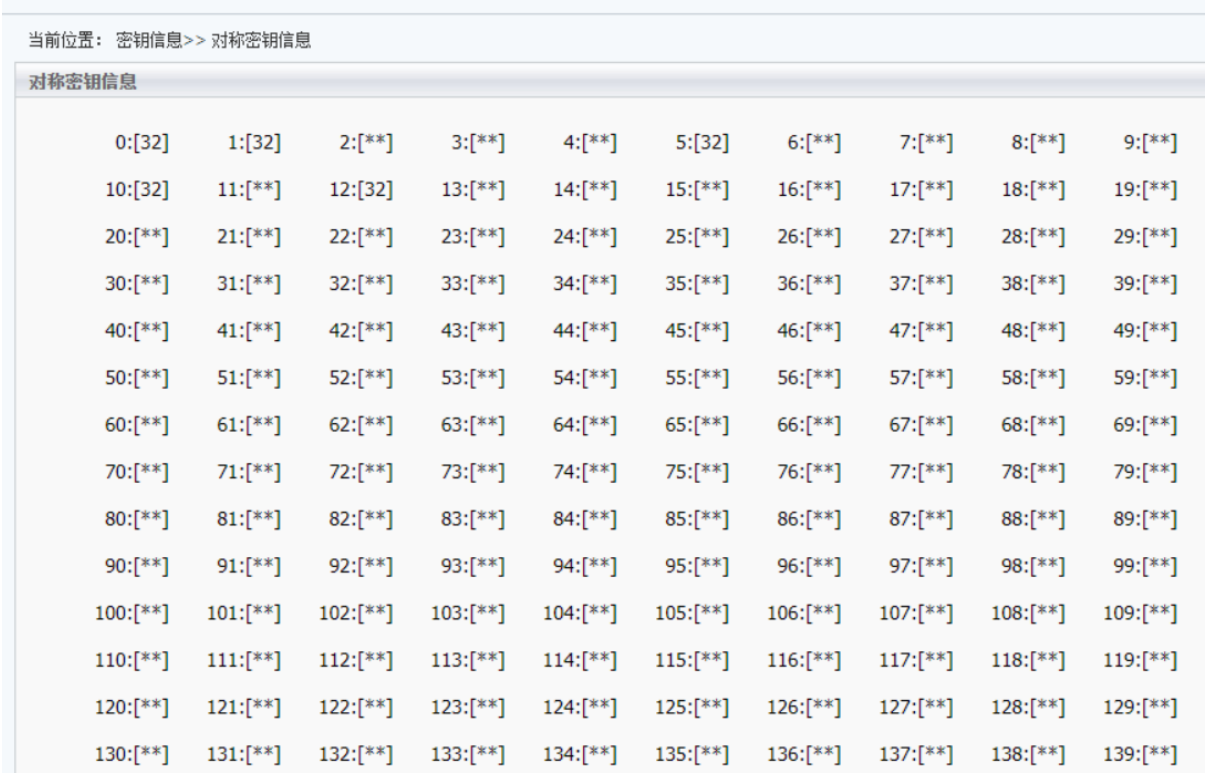
当前位置： 密钥信息>> 对称密钥信息
对称密钥信息
0:[32] 1:[32] 2:[**] 3:[**] 4:[**] 5:[32] 6:[**] 7:[**] 8:[**] 9:[**]
10:[32] 11:[**] 12:[32] 13:[**] 14:[**] 15:[**] 16:[**] 17:[**] 18:[**] 19:[**]
20:[**] 21:[**] 22:[**] 23:[**] 24:[**] 25:[**] 26:[**] 27:[**] 28:[**] 29:[**]
30:[**] 31:[**] 32:[**] 33:[**] 34:[**] 35:[**] 36:[**] 37:[**] 38:[**] 39:[**]
40:[**] 41:[**] 42:[**] 43:[**] 44:[**] 45:[**] 46:[**] 47:[**] 48:[**] 49:[**]
50:[**] 51:[**] 52:[**] 53:[**] 54:[**] 55:[**] 56:[**] 57:[**] 58:[**] 59:[**]
60:[**] 61:[**] 62:[**] 63:[**] 64:[**] 65:[**] 66:[**] 67:[**] 68:[**] 69:[**]
70:[**] 71:[**] 72:[**] 73:[**] 74:[**] 75:[**] 76:[**] 77:[**] 78:[**] 79:[**]
80:[**] 81:[**] 82:[**] 83:[**] 84:[**] 85:[**] 86:[**] 87:[**] 88:[**] 89:[**]
90:[**] 91:[**] 92:[**] 93:[**] 94:[**] 95:[**] 96:[**] 97:[**] 98:[**] 99:[**]
100:[**] 101:[**] 102:[**] 103:[**] 104:[**] 105:[**] 106:[**] 107:[**] 108:[**] 109:[**]
110:[**] 111:[**] 112:[**] 113:[**] 114:[**] 115:[**] 116:[**] 117:[**] 118:[**] 119:[**]
120:[**] 121:[**] 122:[**] 123:[**] 124:[**] 125:[**] 126:[**] 127:[**] 128:[**] 129:[**]
130:[**] 131:[**] 132:[**] 133:[**] 134:[**] 135:[**] 136:[**] 137:[**] 138:[**] 139:[**]

图 25

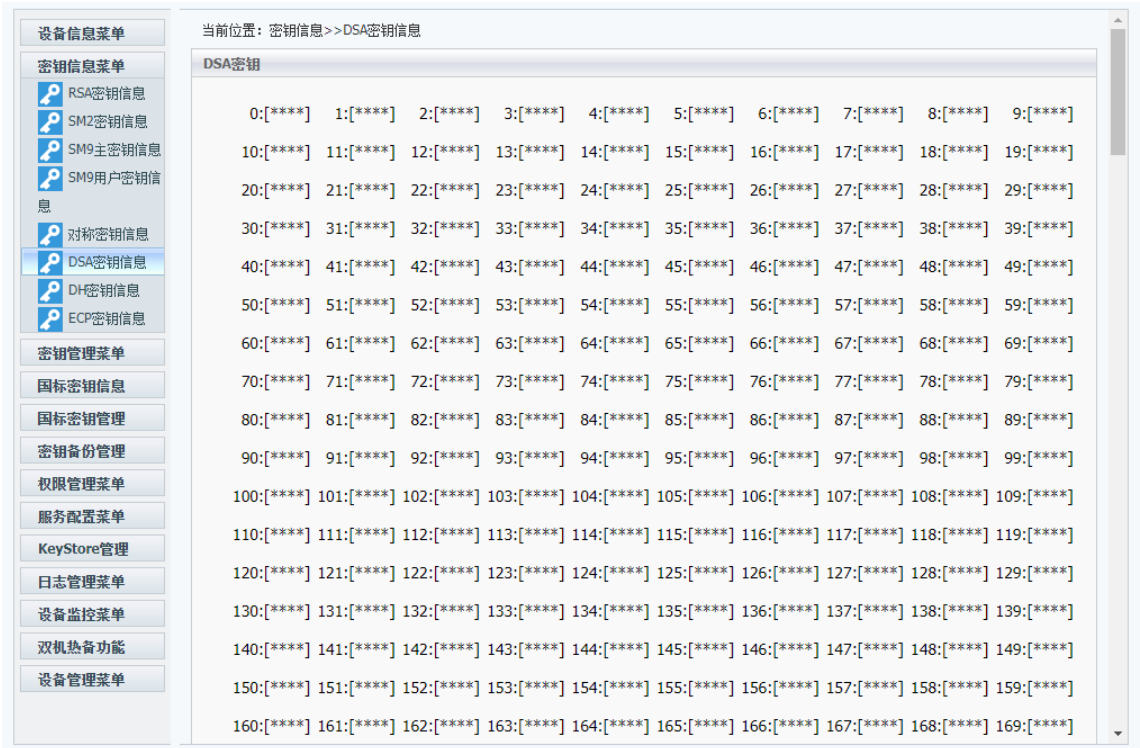
设备信息菜单
密钥信息菜单
RSA密钥信息
SM2密钥信息
SM9主密钥信息
SM9用户密钥信息
对称密钥信息
DSA密钥信息
DH密钥信息
ECP密钥信息
密钥管理菜单
国标密钥信息
国标密钥管理
密钥备份管理
权限管理菜单
服务配置菜单
KeyStore管理
日志管理菜单
设备监控菜单
双机热备功能
设备管理菜单
当前位置：密钥信息>>DSA密钥信息
DSA密钥
0:[****] 1:[****] 2:[****] 3:[****] 4:[****] 5:[****] 6:[****] 7:[****] 8:[****] 9:[****]
10:[****] 11:[****] 12:[****] 13:[****] 14:[****] 15:[****] 16:[****] 17:[****] 18:[****] 19:[****]
20:[****] 21:[****] 22:[****] 23:[****] 24:[****] 25:[****] 26:[****] 27:[****] 28:[****] 29:[****]
30:[****] 31:[****] 32:[****] 33:[****] 34:[****] 35:[****] 36:[****] 37:[****] 38:[****] 39:[****]
40:[****] 41:[****] 42:[****] 43:[****] 44:[****] 45:[****] 46:[****] 47:[****] 48:[****] 49:[****]
50:[****] 51:[****] 52:[****] 53:[****] 54:[****] 55:[****] 56:[****] 57:[****] 58:[****] 59:[****]
60:[****] 61:[****] 62:[****] 63:[****] 64:[****] 65:[****] 66:[****] 67:[****] 68:[****] 69:[****]
70:[****] 71:[****] 72:[****] 73:[****] 74:[****] 75:[****] 76:[****] 77:[****] 78:[****] 79:[****]
80:[****] 81:[****] 82:[****] 83:[****] 84:[****] 85:[****] 86:[****] 87:[****] 88:[****] 89:[****]
90:[****] 91:[****] 92:[****] 93:[****] 94:[****] 95:[****] 96:[****] 97:[****] 98:[****] 99:[****]
100:[****] 101:[****] 102:[****] 103:[****] 104:[****] 105:[****] 106:[****] 107:[****] 108:[****] 109:[****]
110:[****] 111:[****] 112:[****] 113:[****] 114:[****] 115:[****] 116:[****] 117:[****] 118:[****] 119:[****]
120:[****] 121:[****] 122:[****] 123:[****] 124:[****] 125:[****] 126:[****] 127:[****] 128:[****] 129:[****]
130:[****] 131:[****] 132:[****] 133:[****] 134:[****] 135:[****] 136:[****] 137:[****] 138:[****] 139:[****]
140:[****] 141:[****] 142:[****] 143:[****] 144:[****] 145:[****] 146:[****] 147:[****] 148:[****] 149:[****]
150:[****] 151:[****] 152:[****] 153:[****] 154:[****] 155:[****] 156:[****] 157:[****] 158:[****] 159:[****]
160:[****] 161:[****] 162:[****] 163:[****] 164:[****] 165:[****] 166:[****] 167:[****] 168:[****] 169:[****]

图 26

.

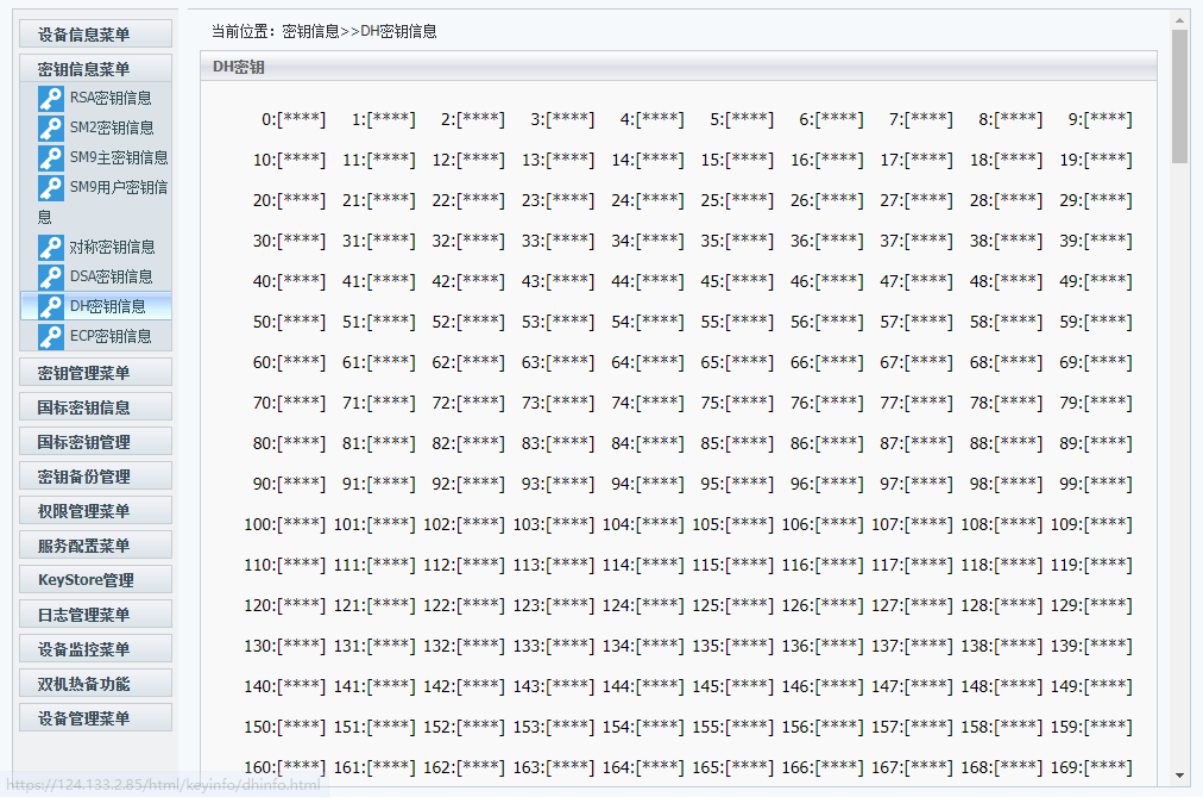
设备信息菜单
密钥信息菜单
RSA密钥信息
SM2密钥信息
SM9主密钥信息
SM9用户密钥信息
对称密钥信息
DSA密钥信息
DH密钥信息
ECP密钥信息
密钥管理菜单
国标密钥信息
国标密钥管理
密钥备份管理
权限管理菜单
服务配置菜单
KeyStore管理
日志管理菜单
设备监控菜单
双机热备功能
设备管理菜单
当前位置：密钥信息>>DH密钥信息
DH密钥
0:[****] 1:[****] 2:[****] 3:[****] 4:[****] 5:[****] 6:[****] 7:[****] 8:[****] 9:[****]
10:[****] 11:[****] 12:[****] 13:[****] 14:[****] 15:[****] 16:[****] 17:[****] 18:[****] 19:[****]
20:[****] 21:[****] 22:[****] 23:[****] 24:[****] 25:[****] 26:[****] 27:[****] 28:[****] 29:[****]
30:[****] 31:[****] 32:[****] 33:[****] 34:[****] 35:[****] 36:[****] 37:[****] 38:[****] 39:[****]
40:[****] 41:[****] 42:[****] 43:[****] 44:[****] 45:[****] 46:[****] 47:[****] 48:[****] 49:[****]
50:[****] 51:[****] 52:[****] 53:[****] 54:[****] 55:[****] 56:[****] 57:[****] 58:[****] 59:[****]
60:[****] 61:[****] 62:[****] 63:[****] 64:[****] 65:[****] 66:[****] 67:[****] 68:[****] 69:[****]
70:[****] 71:[****] 72:[****] 73:[****] 74:[****] 75:[****] 76:[****] 77:[****] 78:[****] 79:[****]
80:[****] 81:[****] 82:[****] 83:[****] 84:[****] 85:[****] 86:[****] 87:[****] 88:[****] 89:[****]
90:[****] 91:[****] 92:[****] 93:[****] 94:[****] 95:[****] 96:[****] 97:[****] 98:[****] 99:[****]
100:[****] 101:[****] 102:[****] 103:[****] 104:[****] 105:[****] 106:[****] 107:[****] 108:[****] 109:[****]
110:[****] 111:[****] 112:[****] 113:[****] 114:[****] 115:[****] 116:[****] 117:[****] 118:[****] 119:[****]
120:[****] 121:[****] 122:[****] 123:[****] 124:[****] 125:[****] 126:[****] 127:[****] 128:[****] 129:[****]
130:[****] 131:[****] 132:[****] 133:[****] 134:[****] 135:[****] 136:[****] 137:[****] 138:[****] 139:[****]
140:[****] 141:[****] 142:[****] 143:[****] 144:[****] 145:[****] 146:[****] 147:[****] 148:[****] 149:[****]
150:[****] 151:[****] 152:[****] 153:[****] 154:[****] 155:[****] 156:[****] 157:[****] 158:[****] 159:[****]
160:[****] 161:[****] 162:[****] 163:[****] 164:[****] 165:[****] 166:[****] 167:[****] 168:[****] 169:[****]

图 27

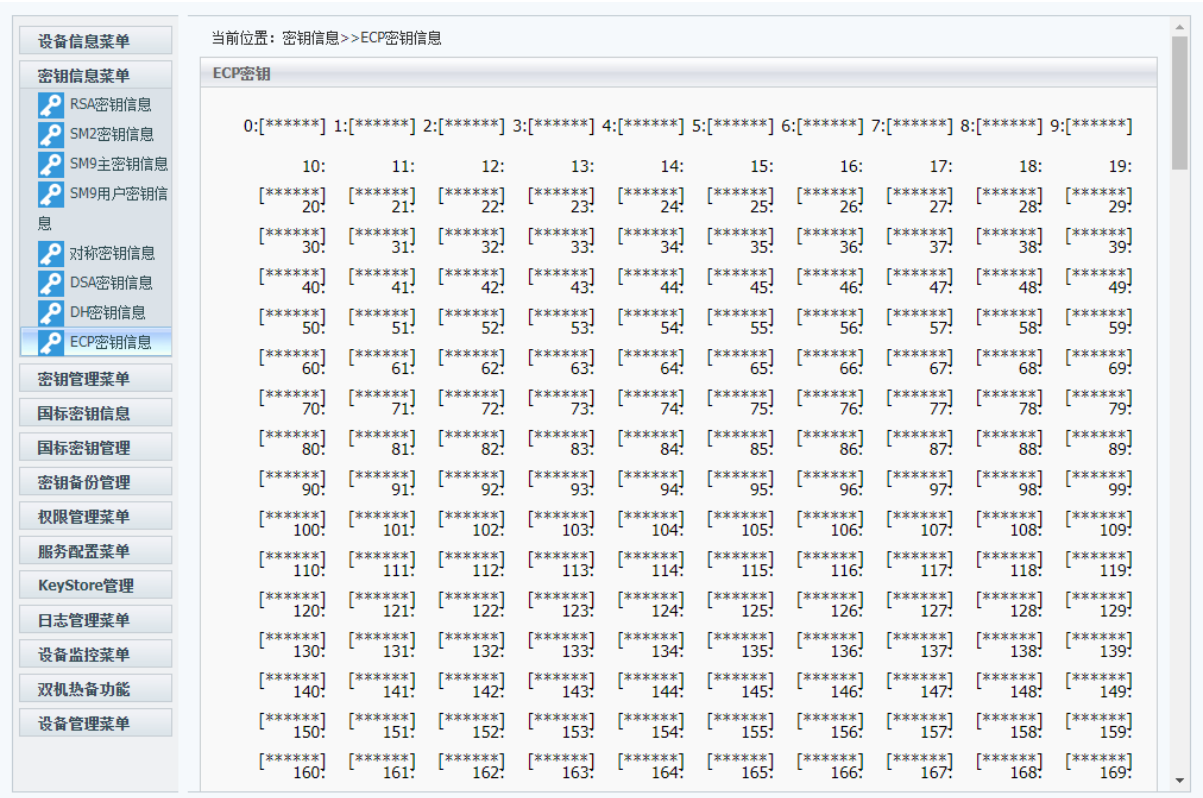
设备信息菜单
密钥信息菜单
RSA密钥信息
SM2密钥信息
SM9主密钥信息
SM9用户密钥信息
对称密钥信息
DSA密钥信息
DH密钥信息
ECP密钥信息
密钥管理菜单
国标密钥信息
国标密钥管理
密钥备份管理
权限管理菜单
服务配置菜单
KeyStore管理
日志管理菜单
设备监控菜单
双机热备功能
设备管理菜单
当前位置：密钥信息>>ECP密钥信息
ECP密钥
0:[******] 1:[******] 2:[******] 3:[******] 4:[******] 5:[******] 6:[******] 7:[******] 8:[******] 9:[******]
10:[******] 11:[******] 12:[******] 13:[******] 14:[******] 15:[******] 16:[******] 17:[******] 18:[******] 19:[******]
20:[******] 21:[******] 22:[******] 23:[******] 24:[******] 25:[******] 26:[******] 27:[******] 28:[******] 29:[******]
30:[******] 31:[******] 32:[******] 33:[******] 34:[******] 35:[******] 36:[******] 37:[******] 38:[******] 39:[******]
40:[******] 41:[******] 42:[******] 43:[******] 44:[******] 45:[******] 46:[******] 47:[******] 48:[******] 49:[******]
50:[******] 51:[******] 52:[******] 53:[******] 54:[******] 55:[******] 56:[******] 57:[******] 58:[******] 59:[******]
60:[******] 61:[******] 62:[******] 63:[******] 64:[******] 65:[******] 66:[******] 67:[******] 68:[******] 69:[******]
70:[******] 71:[******] 72:[******] 73:[******] 74:[******] 75:[******] 76:[******] 77:[******] 78:[******] 79:[******]
80:[******] 81:[******] 82:[******] 83:[******] 84:[******] 85:[******] 86:[******] 87:[******] 88:[******] 89:[******]
90:[******] 91:[******] 92:[******] 93:[******] 94:[******] 95:[******] 96:[******] 97:[******] 98:[******] 99:[******]
100:[******] 101:[******] 102:[******] 103:[******] 104:[******] 105:[******] 106:[******] 107:[******] 108:[******] 109:[******]
110:[******] 111:[******] 112:[******] 113:[******] 114:[******] 115:[******] 116:[******] 117:[******] 118:[******] 119:[******]
120:[******] 121:[******] 122:[******] 123:[******] 124:[******] 125:[******] 126:[******] 127:[******] 128:[******] 129:[******]
130:[******] 131:[******] 132:[******] 133:[******] 134:[******] 135:[******] 136:[******] 137:[******] 138:[******] 139:[******]
140:[******] 141:[******] 142:[******] 143:[******] 144:[******] 145:[******] 146:[******] 147:[******] 148:[******] 149:[******]
150:[******] 151:[******] 152:[******] 153:[******] 154:[******] 155:[******] 156:[******] 157:[******] 158:[******] 159:[******]
160:[******] 161:[******] 162:[******] 163:[******] 164:[******] 165:[******] 166:[******] 167:[******] 168:[******] 169:[******]

图 28

单击左侧菜单栏“国标密钥信息”按钮，进入密钥信息查看页面，查看国标格式的RSA密钥、SM2密钥、对称密钥，如图29-30。

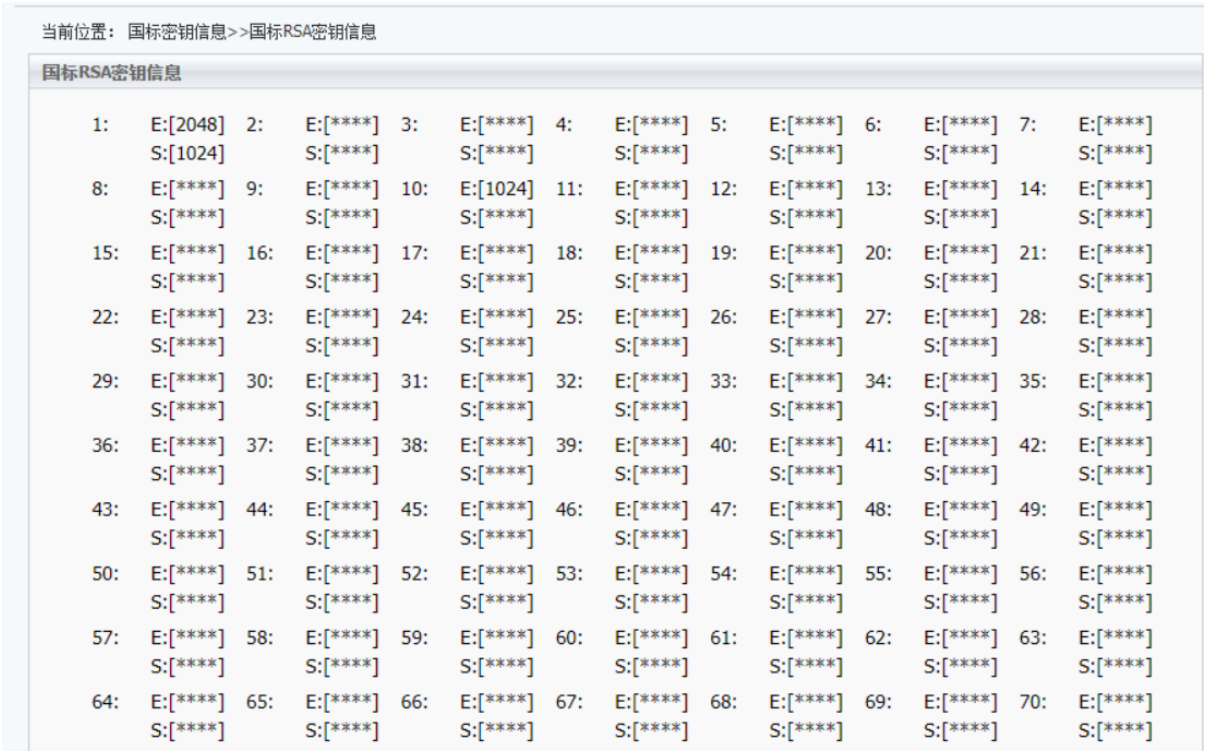

图 29

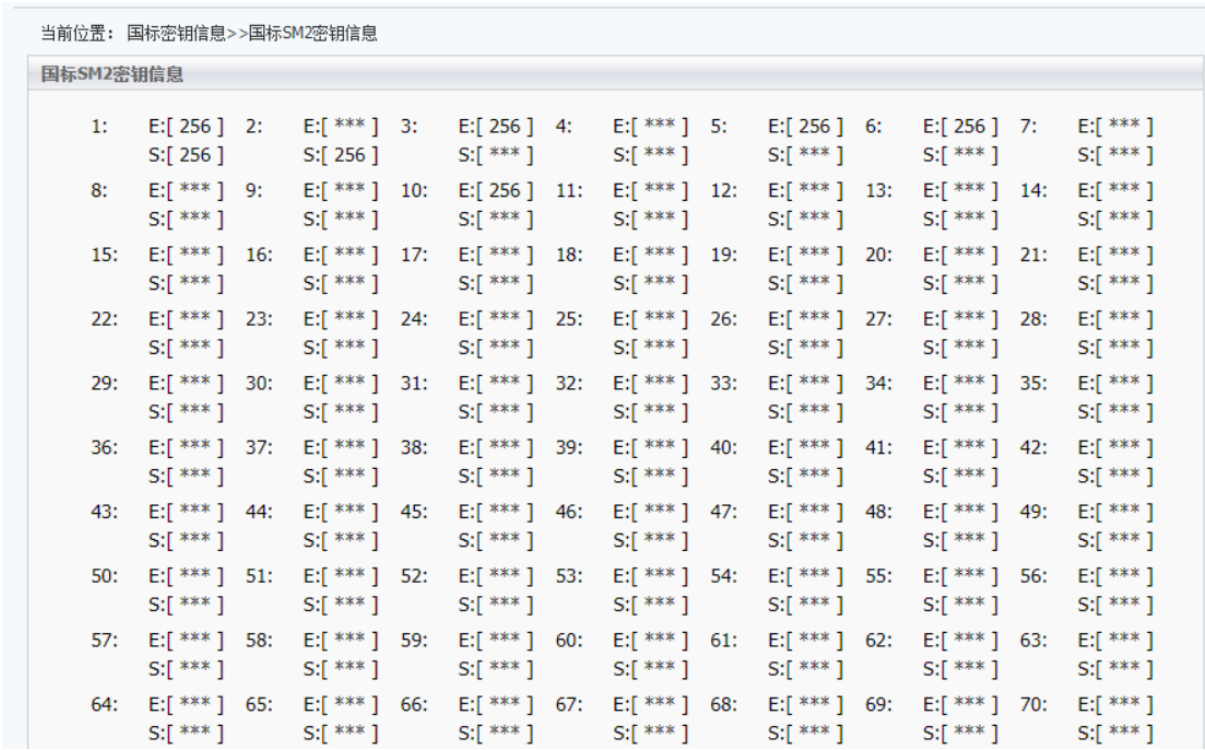

图 30

3.4 服务器密码机秘钥管理

3.4.1 设备主密钥更新

单击左侧菜单栏“密钥管理”，并单击“管理密钥”按钮，如图31。单击网页中“管理密钥初始化”按钮，完成密钥初始化。设置设备主密钥需要满足管理员权限。

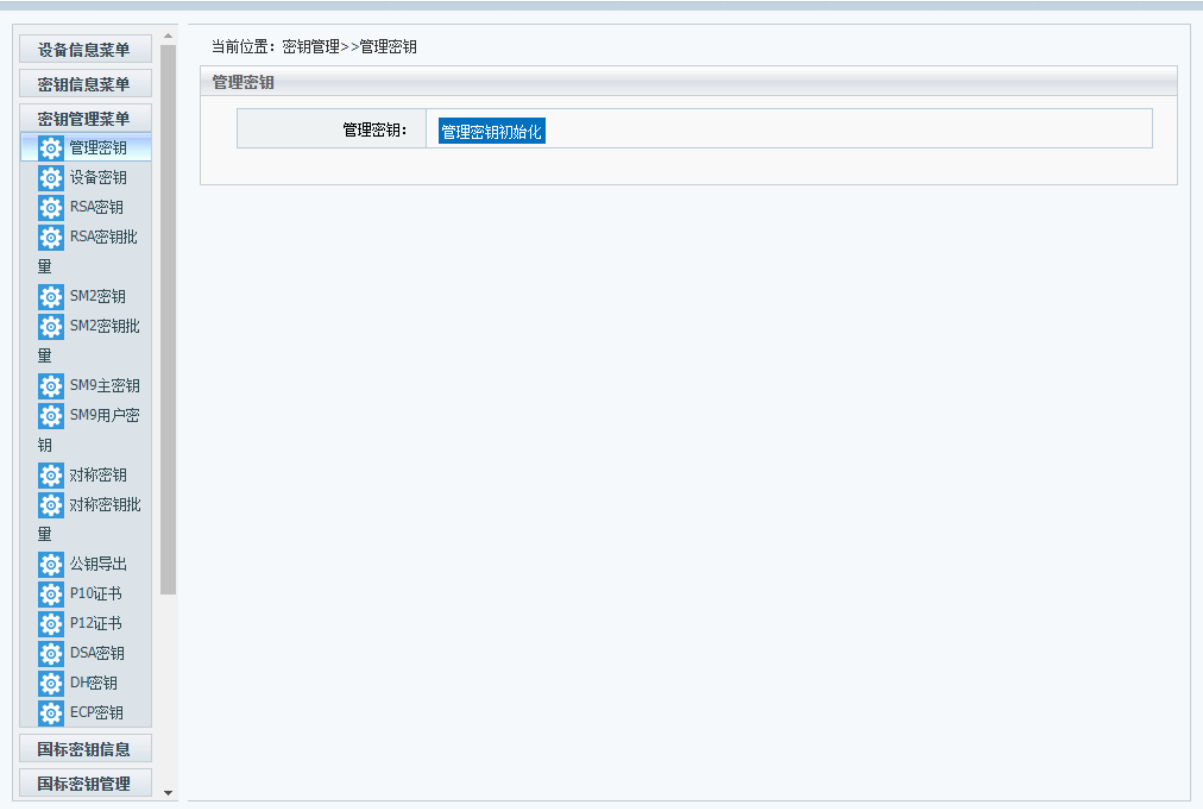

图 31

3.4.2 RSA密钥添加/删除

对密钥的添加、删除操作，需要满足管理员权限。

单击左侧菜单栏“密钥管理”按钮，进入“RSA密钥”页面如图32。输入密钥号并选择模长，可进行RSA密钥的生成与删除。

图 32

单击左侧菜单栏“密钥管理”按钮，进入“RSA密钥批量”界面如图33。输入密钥号范围，选择模长之后，可进行RSA密钥的批量生成与删除。

图 33

3.4.3 SM2密钥添加/删除

对密钥的添加、删除操作，需要满足管理员权限。

单击左侧菜单栏“密钥管理”按钮，进入“SM2密钥”页面如图34。输入密钥号可进行SM2密钥的生成与删除。

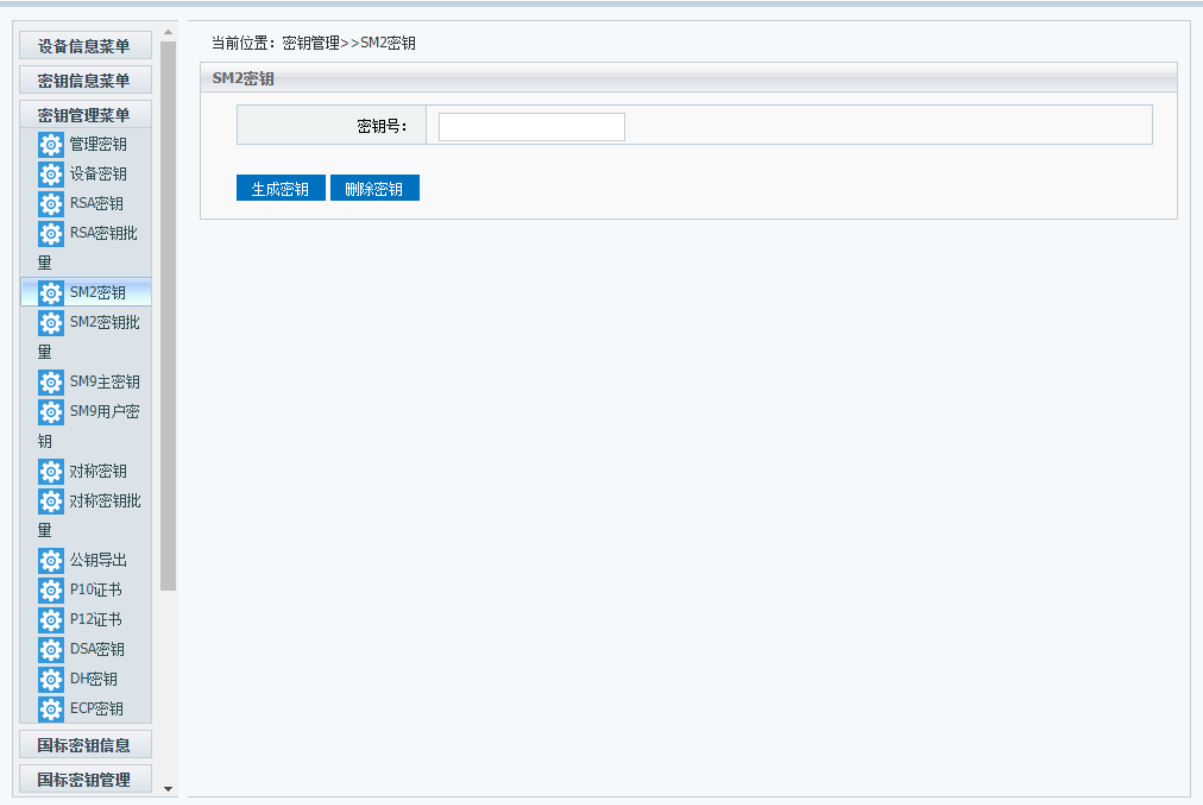

图 34

单击左侧菜单栏“密钥管理”按钮，进入“SM2密钥批量”界面如图35。输入密钥号范围可进行SM2密钥的批量生成与删除。

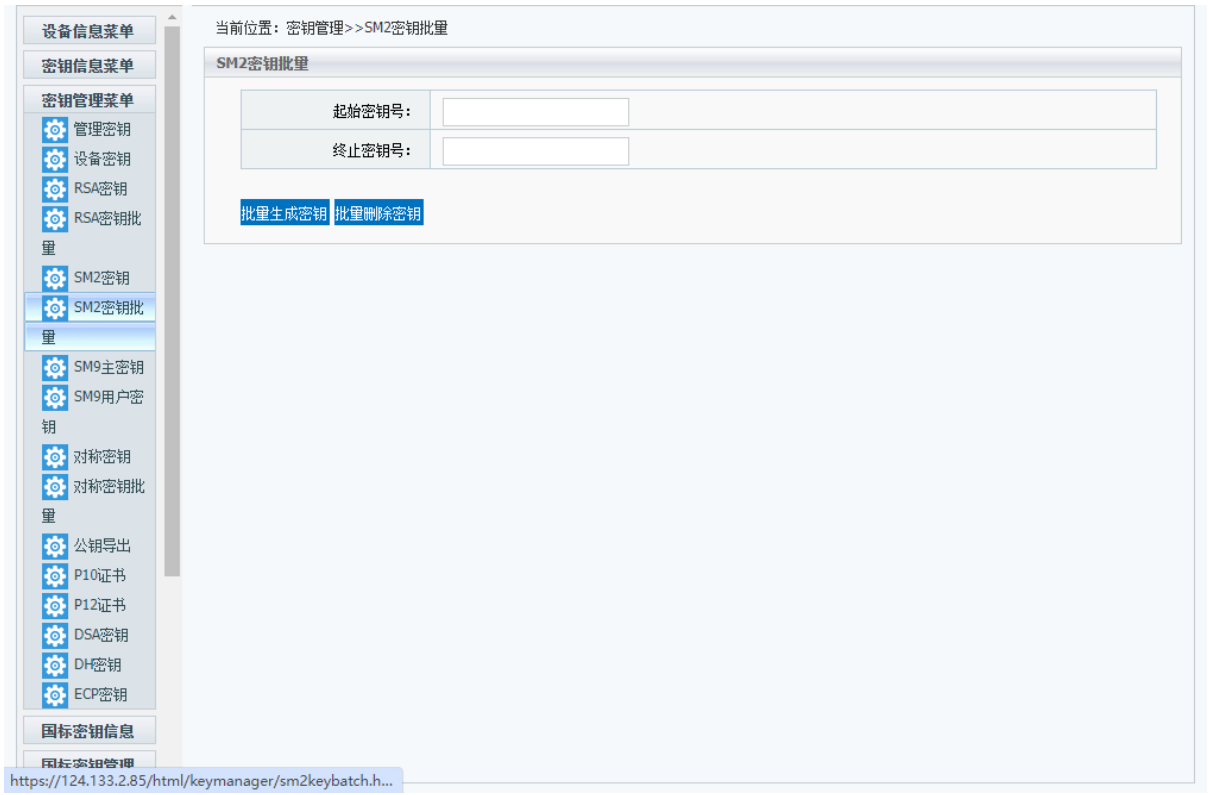

图 35

3.4.4 SM9主密钥添加/删除

SM9主密钥的添加、删除操作，需要满足管理员权限。

单击左侧菜单栏“密钥管理”按钮，进入“SM9主密钥”页面。如果此设备算法类型不支持SM9密钥，则相关菜单选项为灰色，不可操作。如图36所示。

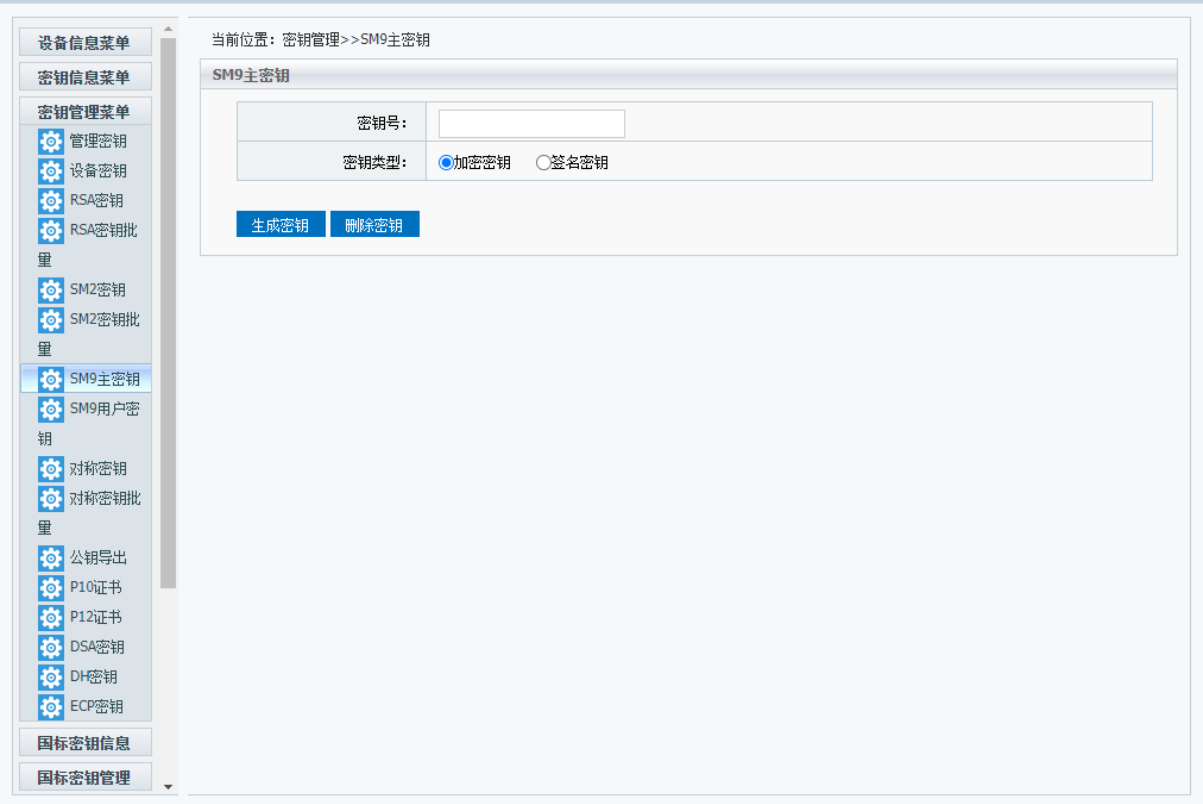

图 36

若此设备算法类型支持SM9密钥操作，在密钥号输入框中输入指定密钥号，密钥类型可以选择加密密钥、签名密钥，单击“添加”按钮，完成SM9主密钥添加；在密钥号输入框中输入指定密钥号，单击“删除”按钮，完成SM9主密钥删除。如图37。

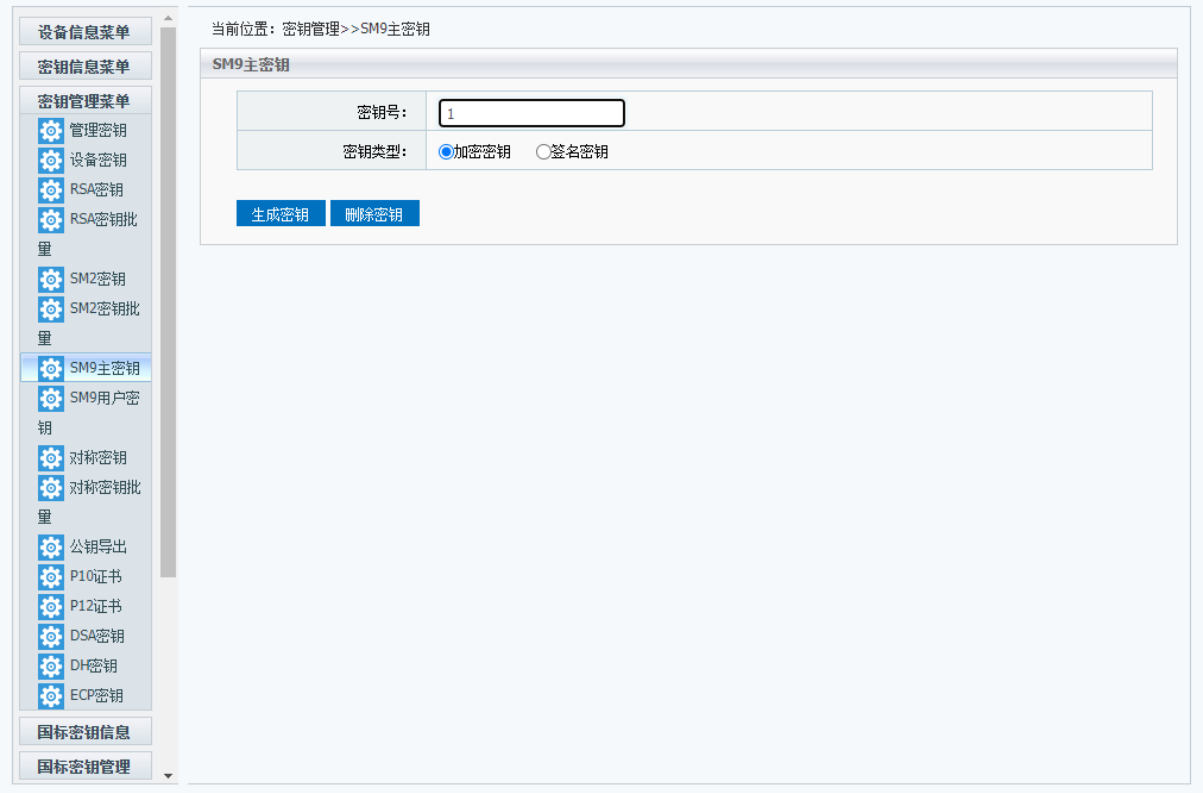

图 37

3.4.5 SM9用户密钥添加/删除

SM9用户密钥的添加、删除操作，需要满足管理员权限。

单击左侧菜单栏“密钥管理”按钮，并单击“SM9用户密钥”按钮，进入SM9用户密钥管理界面。如果此设备算法类型不支持SM9密钥，则相关菜单选项为灰色，不可操作。如图38所示。

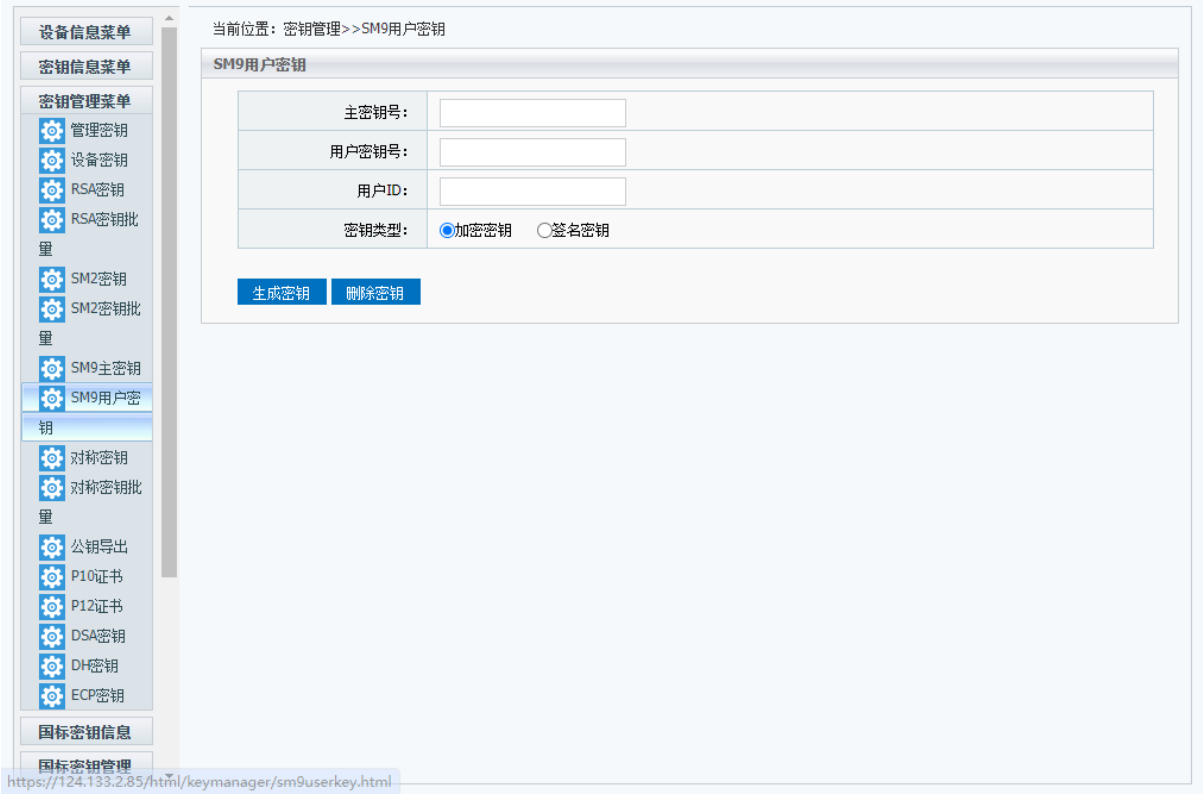

图 38

若此设备支持SM9算法，在密钥号输入框中输入指定主密钥号、用户密钥号、用户id，密钥类型可以选择加密密钥、签名密钥，单击“添加”按钮，完成SM9用户密钥添加；在密钥号输入框中输入指定用户密钥号，单击“删除”按钮，完成SM9用户密钥删除。如图39。

图 39

3.4.6 对称密钥添加/删除

对密钥的添加、删除操作，需要满足管理员权限。

单击左侧菜单栏“密钥管理”按钮，并单击“对称密钥”按钮，如图40。

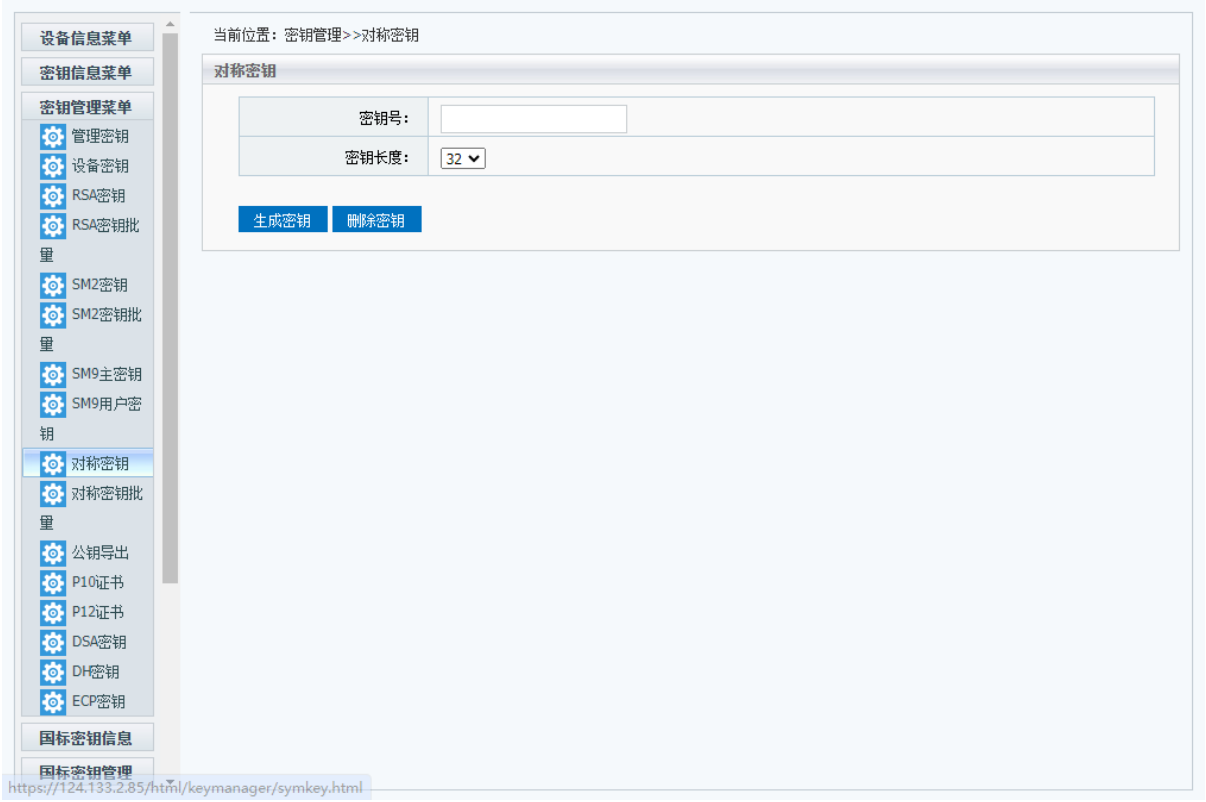

图 40

添加/删除对称密钥时需要满足管理员权限，在密钥号输入框中输入指定密钥号，密钥长度可选择8、16、24、32，单击“添加”按钮，完成对称密钥添加；

在密钥号输入框中输入指定密钥号，单击“删除”按钮，完成对称密钥删除。

单击左侧菜单栏“密钥管理”按钮，进入“对称密钥批量”界面，如图41。输入密钥号范围，并选择号密钥长度可进行密钥的批量生成与删除。

图 41

3.4.7 导出公钥

单击左侧菜单栏“密钥管理”按钮，并单击“公钥导出”按钮，如图42。

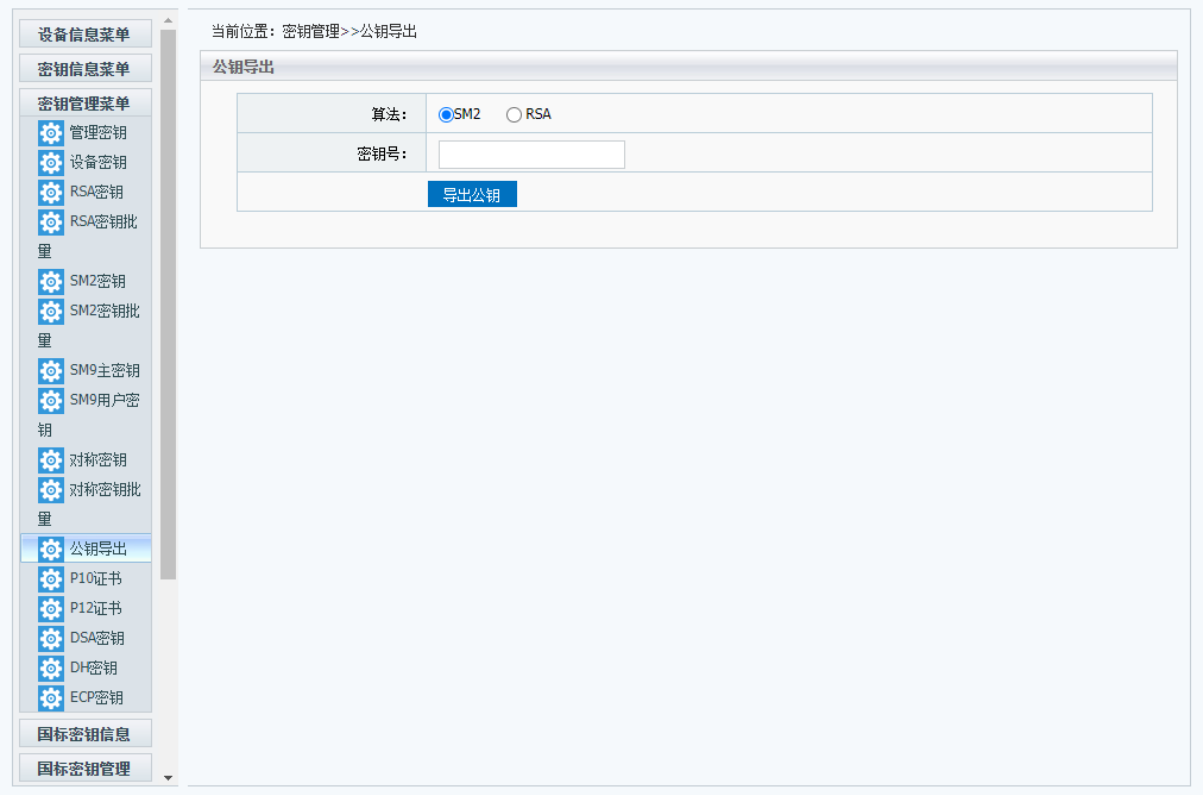

图 42

3.4.8 P10证书

单击左侧菜单栏“密钥管理”按钮，进入“p10证书”管理页面。生成p10的密钥号必须提前生成密钥。然后，选择密钥类型，填写密钥号，并根据实际需要，填写办法对象、国家、省/自治区、县市、单位、部门。并单击“P10证书”按钮，如图43。

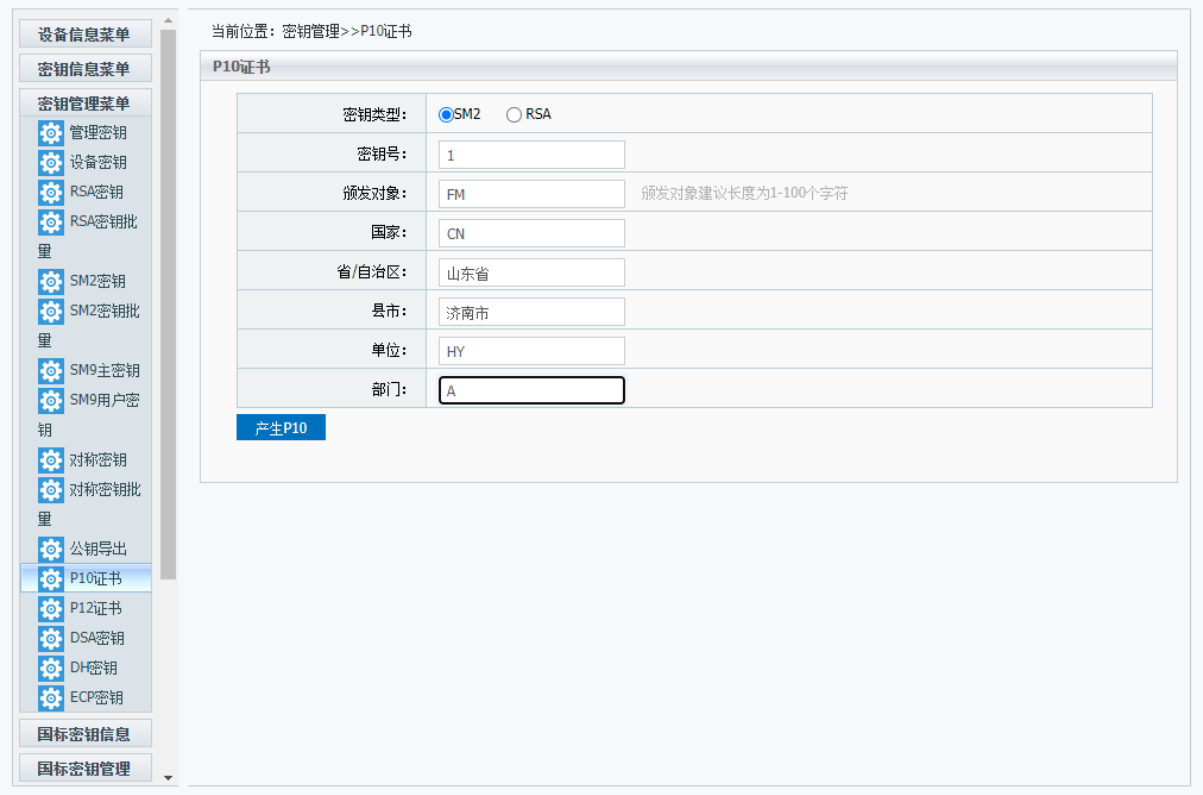

图 43

3.4.9 P12证书

使用P12证书的导入功能可以将P12文件中的密钥导入指定密钥号中。如图44。选择需要导入的密钥号，并填写口令，然后上传p12证书，选择“导入p12证书”。提示导入成功，则对应的密钥类型的密钥号位置会导入p12证书中保存的密钥信息。

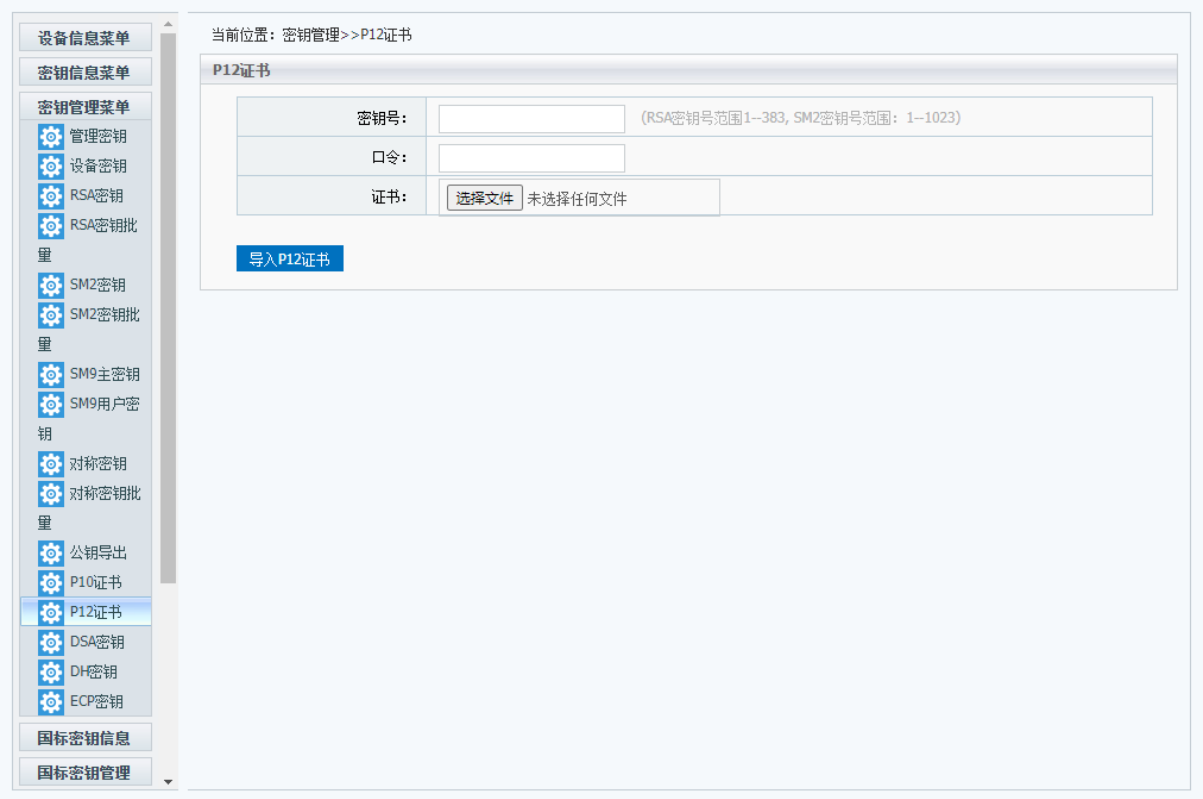

图 44

3.4.10 密钥备份

对密钥的备份操作，需要满足管理员权限。

单击左侧菜单栏“密钥备份”，并单击“密钥备份”按钮，如图45。

图 45

密钥备份操作需要添加五个管理员并登陆。单击“开始备份”按钮，提示“确定开始进行备份吗”，点击确定后，跳转进入“密钥备份”管理页面。如图46。

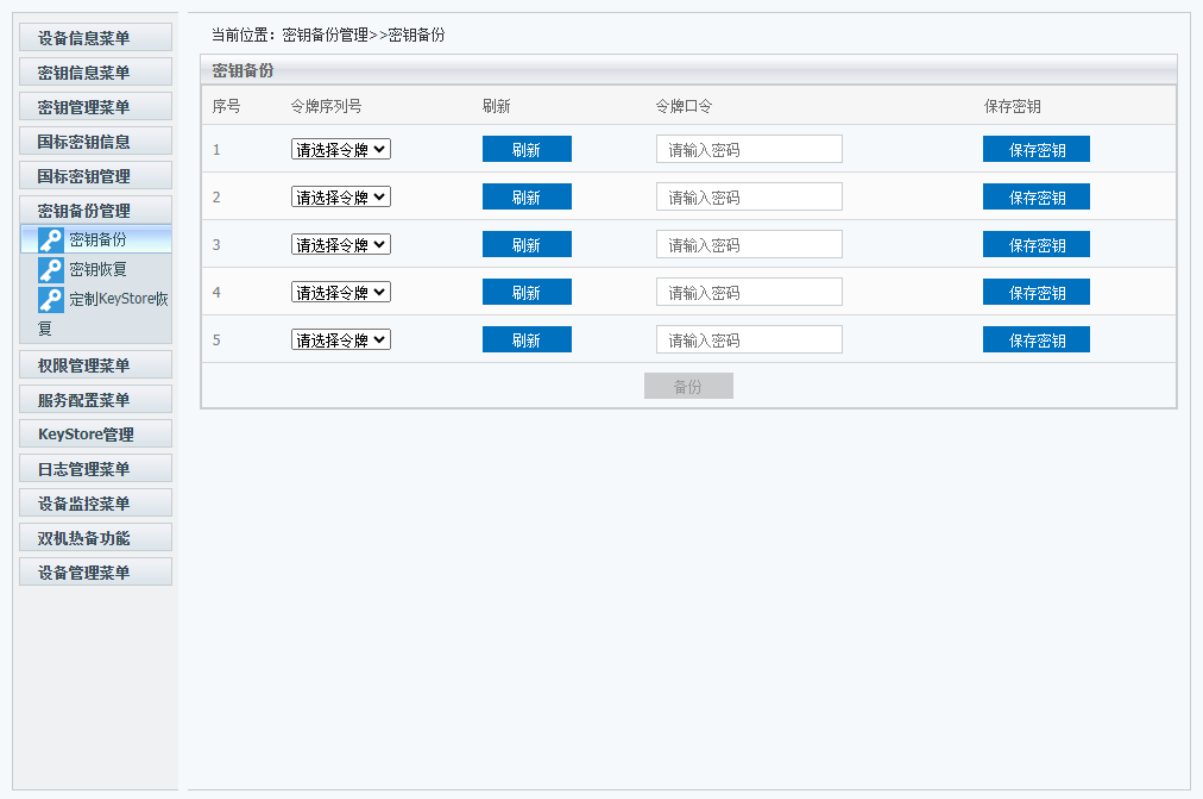

图 46

在配置终端插入USB KEY，输入USB KEY口令，单击保存密钥。提示成功后插入下一个管理员USB KEY，重复此前操作。5个管理员密钥保存完成后，“备份”按钮可以点击，如图47。

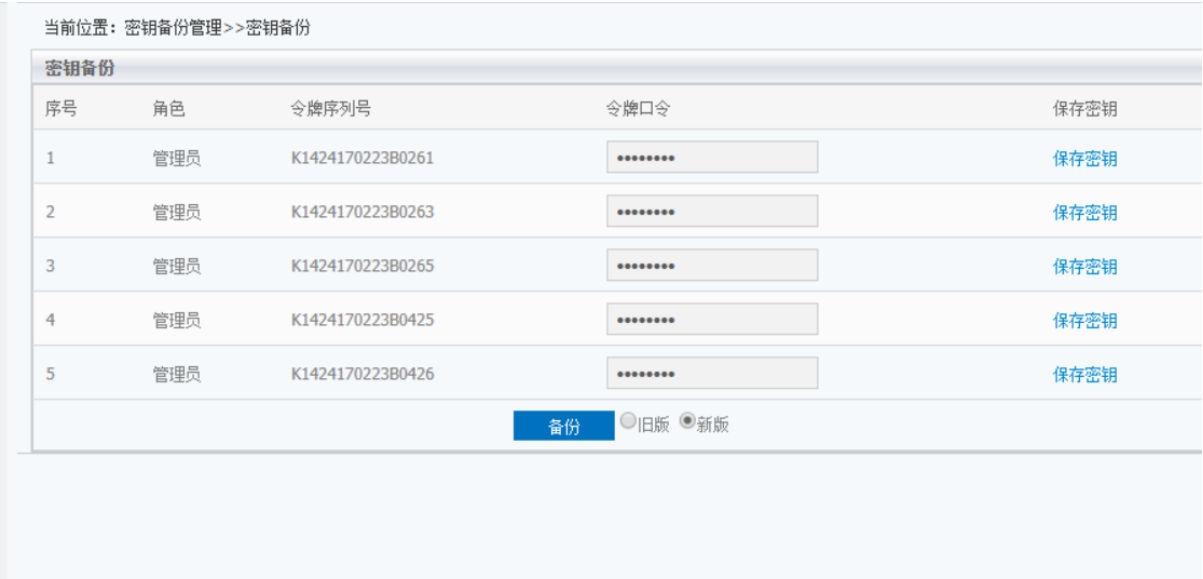

图 47

然后单击“备份”按钮，等待备份完成，提示备份成功，如图48。

图 48

备份时，可选择备份为旧版本，或者新版本。旧版本备份文件兼容2015年之前的加密机服务器。新版本备份文件只能用于2015年之后的加密服务器中。

密钥备份完成后点击“下载备份文件”按钮，如图49，点击“保存”按钮，保存备份文件到主机。请妥善保管该文件。本版本最多支持5次备份文件，用户管理的5把key中只保留最新5次备份文件。

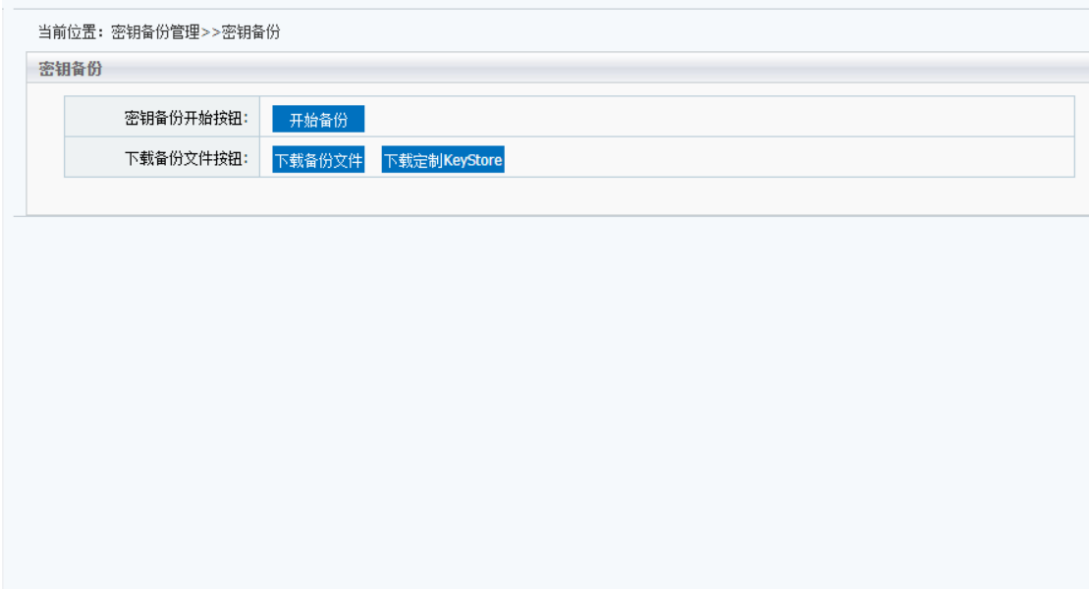

图 49

3.4.11 密钥恢复

单击左侧菜单栏“密钥管理”按钮，并单击“密钥恢复”按钮，如图50。

图 50

在进行密钥恢复功能前，请确认已经登录三个管理员。首先，选择备份文件，从五个管理员KEY中任意选取三个即可完成恢复密钥的操作。在配置终端插入任意一个管理员USB KEY，勾选对应的USB KEY序列号，输入USB KEY口令，单击“取得密钥”按钮，提示成功后，插入下一个USB KEY，重复操作。获取3个密钥片段后，备份文件版本，可以选择对应的备份文件版本，单击“恢复”按钮，如**错误!未找到引用源。**

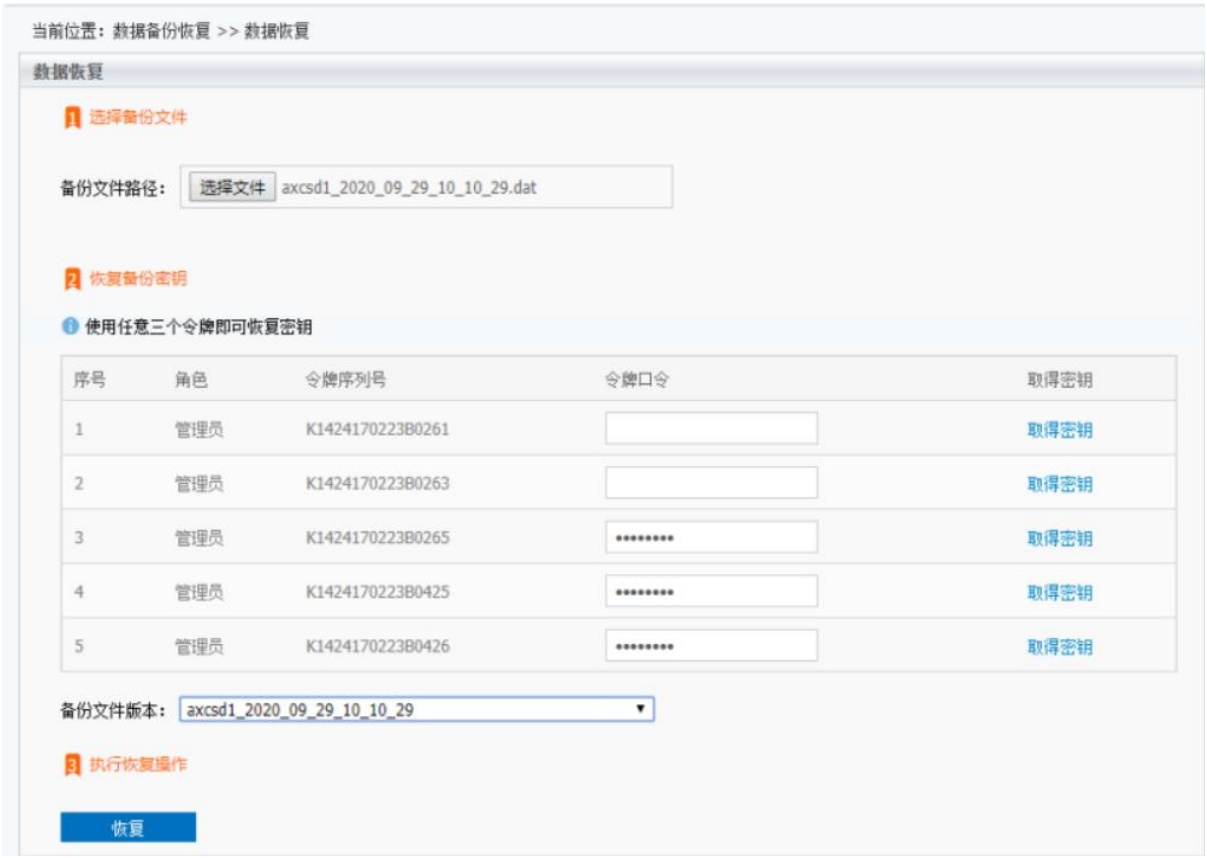

图 51

单击“恢复”进入恢复界面如图52。

图 52

恢复完成，提示恢复成功。如图53。

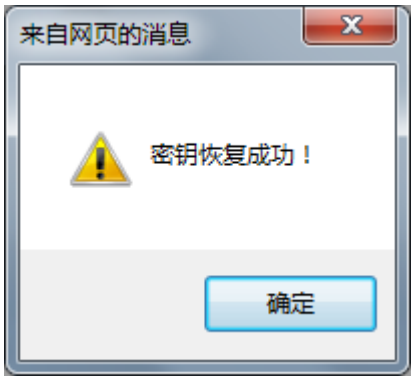

图 53

完成后进入恢复界面，单击“恢复”完成密钥恢复操作。

3.5 服务器密码机KeyStore配置管理

对密码机的KeyStore配置，需要满足管理员权限。

单击左侧菜单栏“KeyStore管理”菜单，并单击“KeyStore配置”菜单，如**错误!未找到引用源。**4。

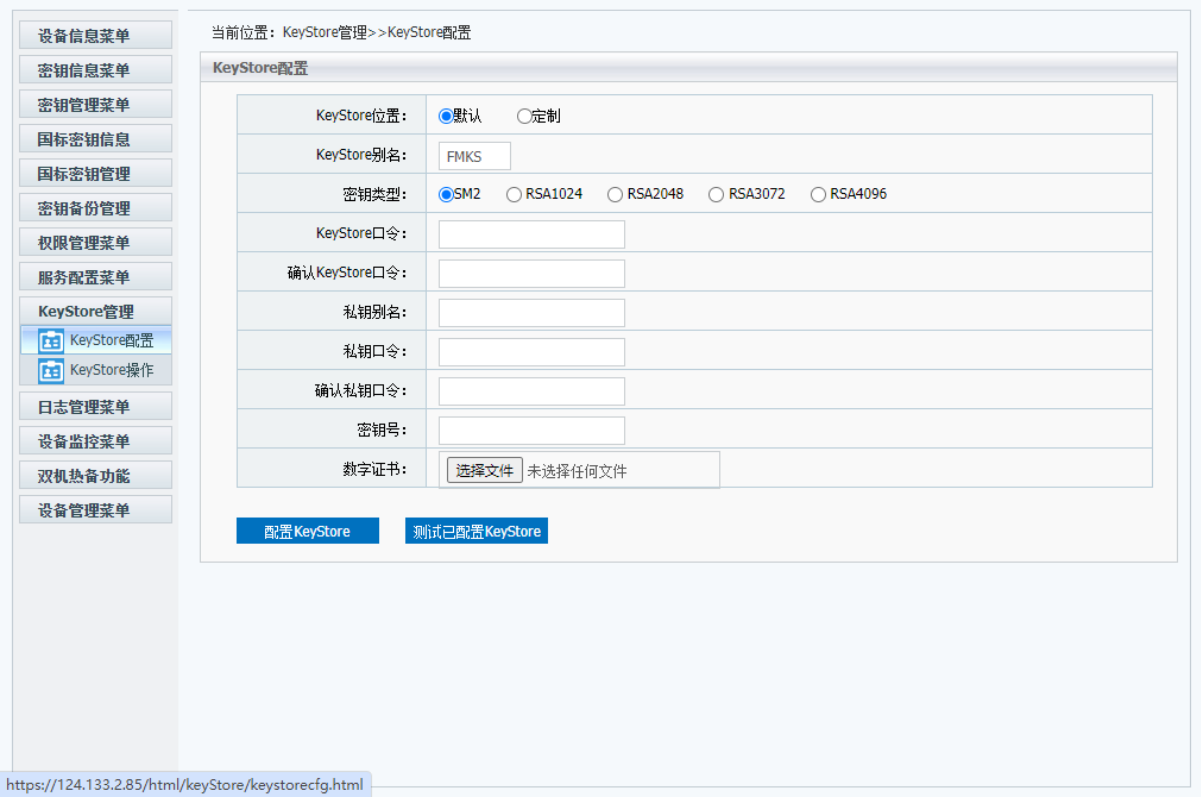

图 54

加密机内的KeyStore分默认和定制两种方式，如果对keystore没有特殊要求，选择默认方式，如果需要keystore扩容，需选择定制方式。默认方式的KeyStore空间只有20K，能够存放的Keystore数据较小，定制方式的KeyStore空间为20M，可以存放较多的数据。客户根据自己的应用需求，灵活选择。KeyStore测试功能可以检查配置是否正确。

通过keystore配置页面，可以对keystore进行枚举、删除、和清空等操作，如图55

图 55

3.6 服务器密码机日志管理

3.6.1 服务器密码机日志设置

单击左侧菜单栏“日志管理”按钮，并单击“日志管理”按钮，如图56。

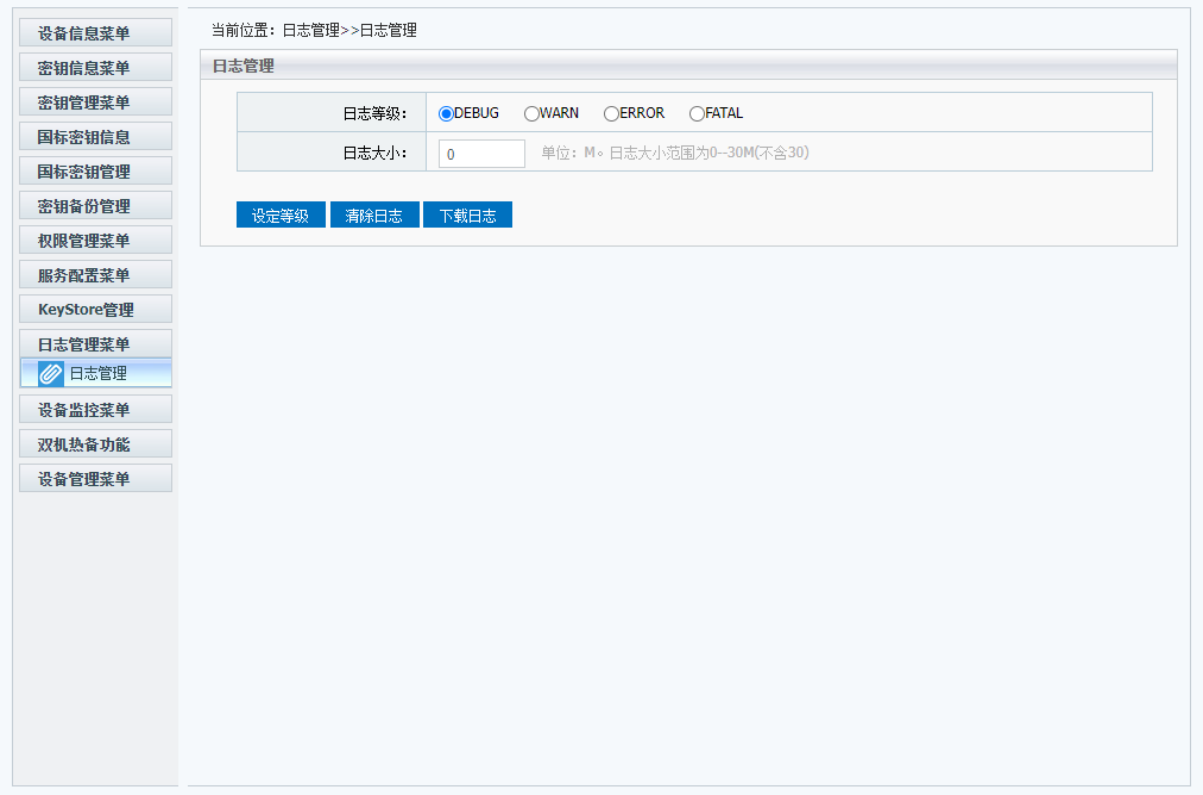

图 56

默认日志等级为ERROR，加密机出错时打日志，日志文件大小默认2M，单击“设置等级”按钮可以修改日志等级和日志大小。单击“清除日志”可以将日志文件删除。单击“下载日志”可以将日志文件下载到本地。

3.6.2 审计查询

进行审计查询是，需要有审计管理员权限。选择开始时间和结束时间后，单击 “查询”按钮，如**错误!未找到引用源。**7。

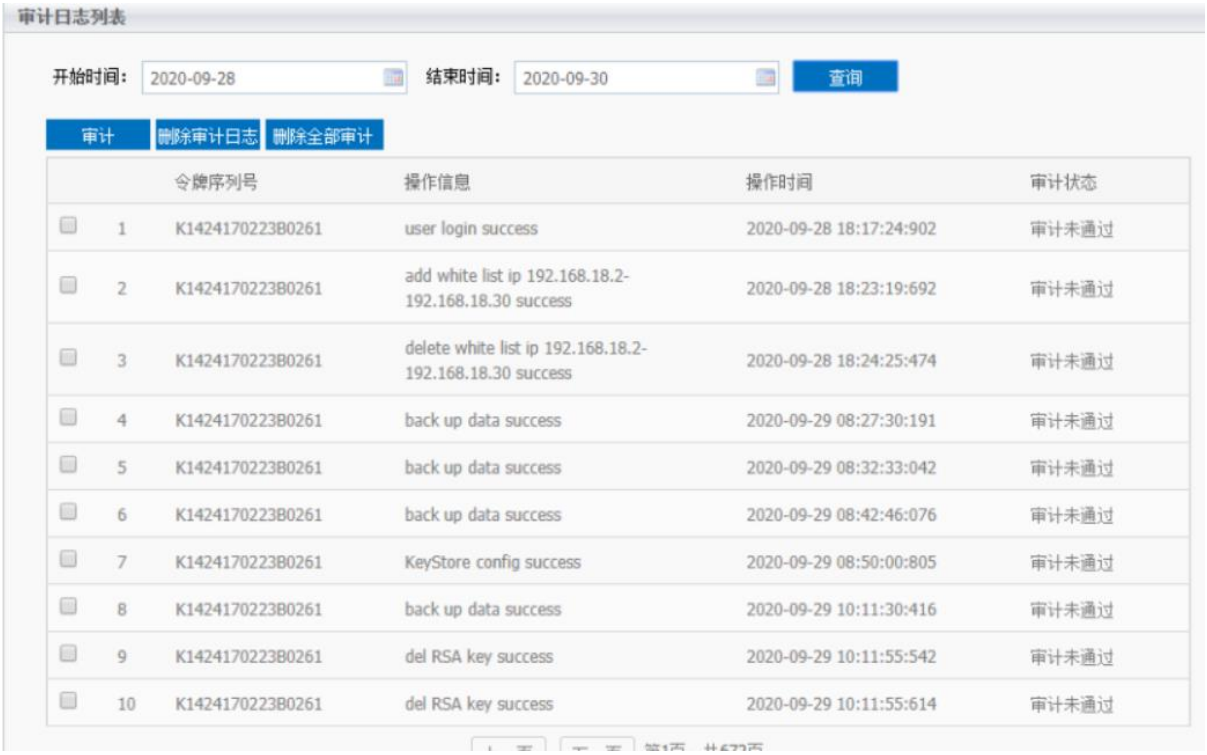

图 57

3.6.3 审计

审计功能需要有审计管理员权限才能进行审计操作。选择需要审计的日志，单击“审计”按钮，审计状态修改为“审计通过”，如图58。

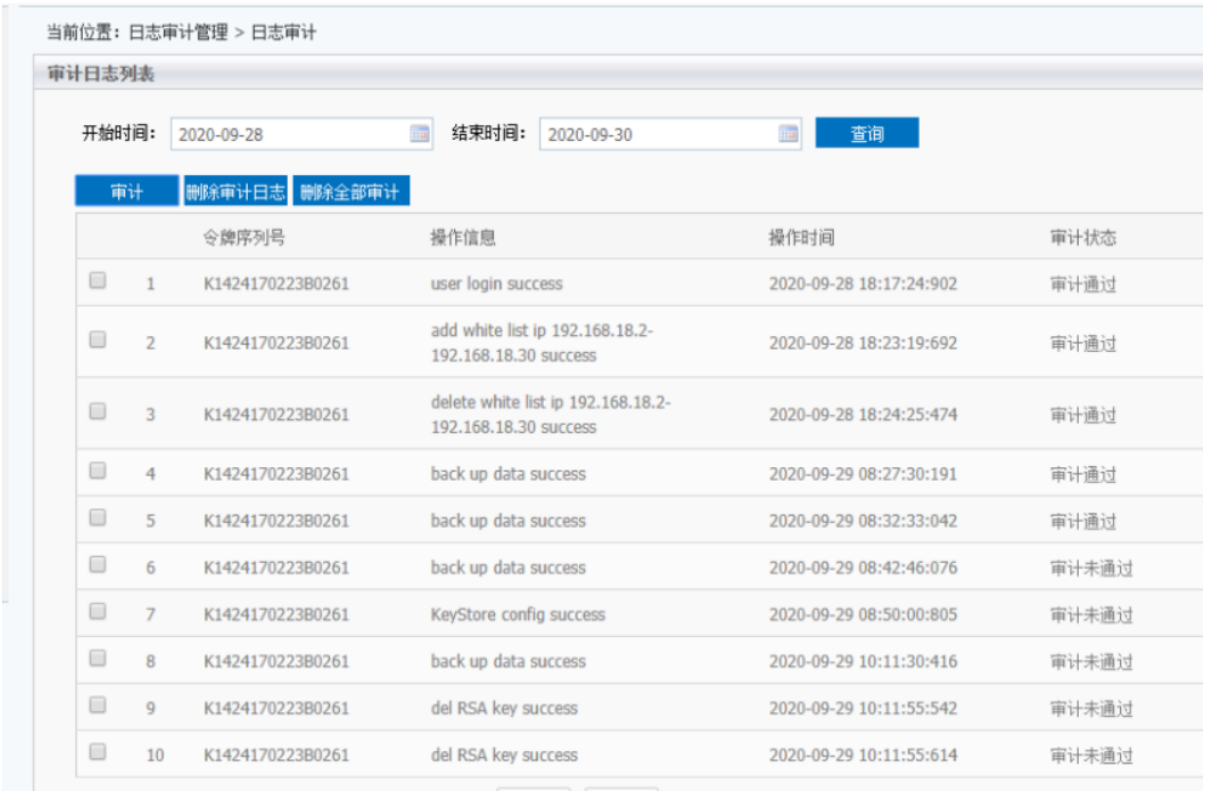

图 58

3.6.4 审计删除

审计删除操作需要有审计管理员权限才能进行。选择需要删除的的日志，单击“删除审计日志”按钮，选中的日志将被删除，如**错误!未找到引用源。**9。

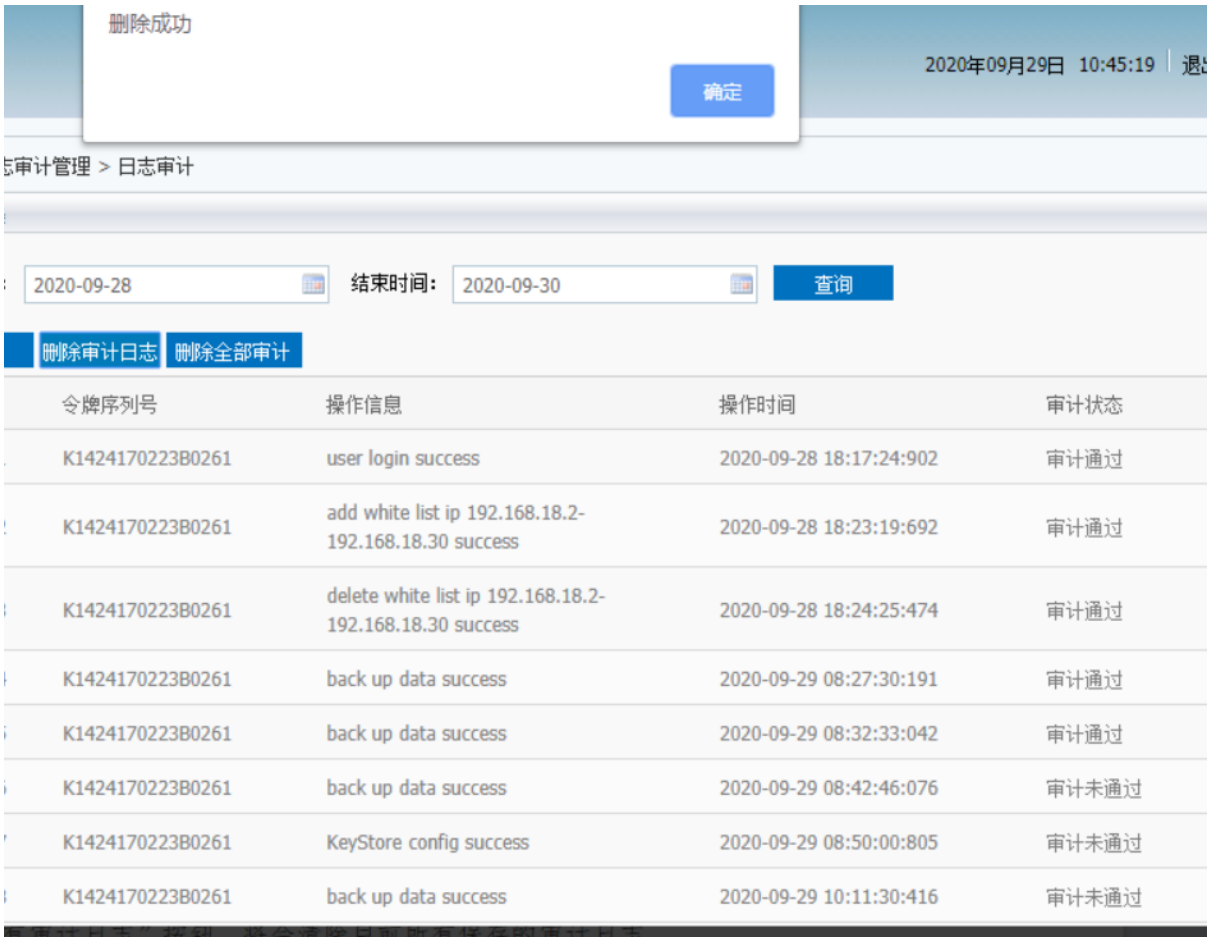

图 59

点击“删除审计日志”按钮，可以逐条删除审计日志。

点击“删除所有审计日志”按钮，将会清除目前所有保存的审计日志。

3.7 服务器密码机监控

服务器密码机当前业务操作监控

单击左侧菜单栏“设备监控”按钮，并单击“监控服务”按钮，如**错误!未找到引用源。**0。

图 60

可以每隔几秒钟看到服务器密码机所作的操作和当前服务器密码机并发连接数目。

3.8 双机热备

双机热备需要两台密码机服务器，一台为主机，一台为从机，正常状态下由主机提供服务，从机保持与主机的数据同步。当主机因故停止运行后，从机自动切换为主机，继续提供服务。主从机的数据同步依赖于网络，所以在使用此功能时务必保持主从机的网络通讯正常。

3.8.1 服务器密码机热备设置

单击左侧菜单栏“双机热备”按钮，并单击“热备设置”按钮，如**错误!未找到引用源。**。

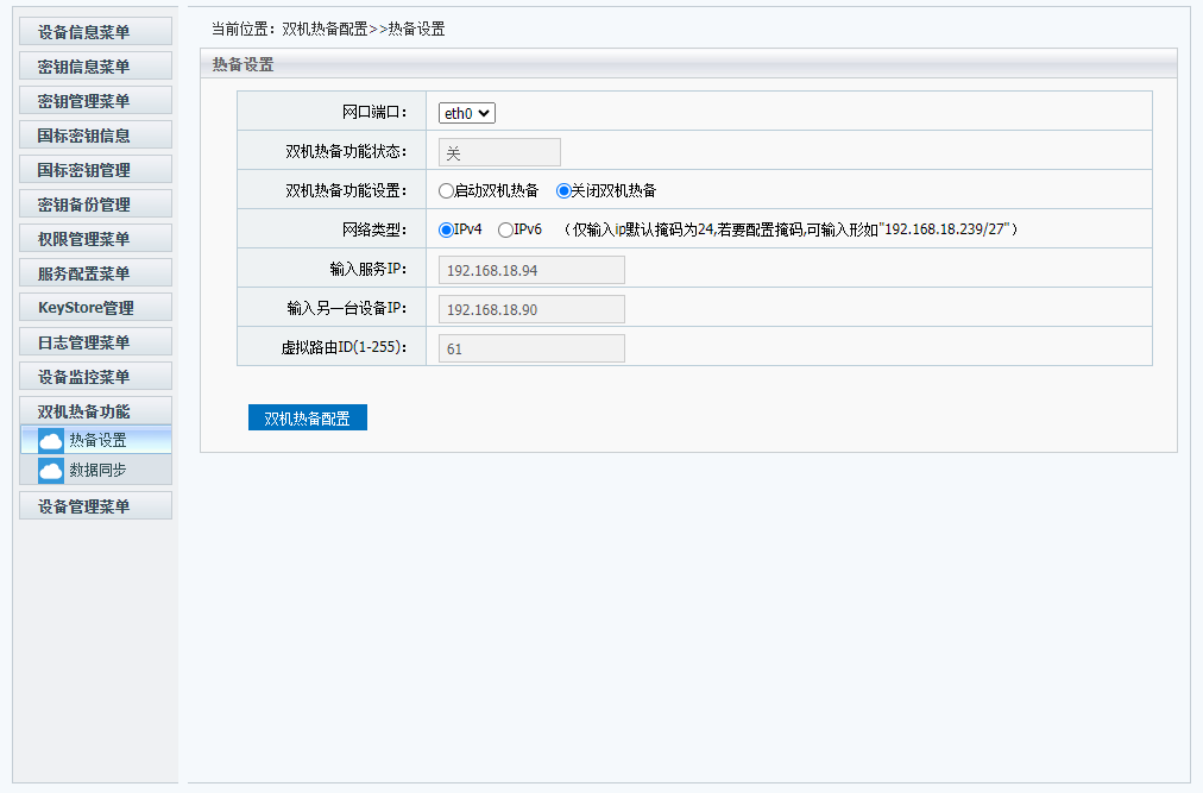

图 61

（一）、开启双击热备功能：

双机热备功能的开启，需要2台加密机A和B配合完成。选中网口端口，输入要进行配置的网口、点击选中 “启动双机热备”；随后输入 服务器 设备IP，另一台机器设备的 IP,虚拟路由ID；点击 “双击热备配置” 按钮 ，来保存配置信息。重启加密机服务器后，双机热备的设置才能生效。如图62所示。

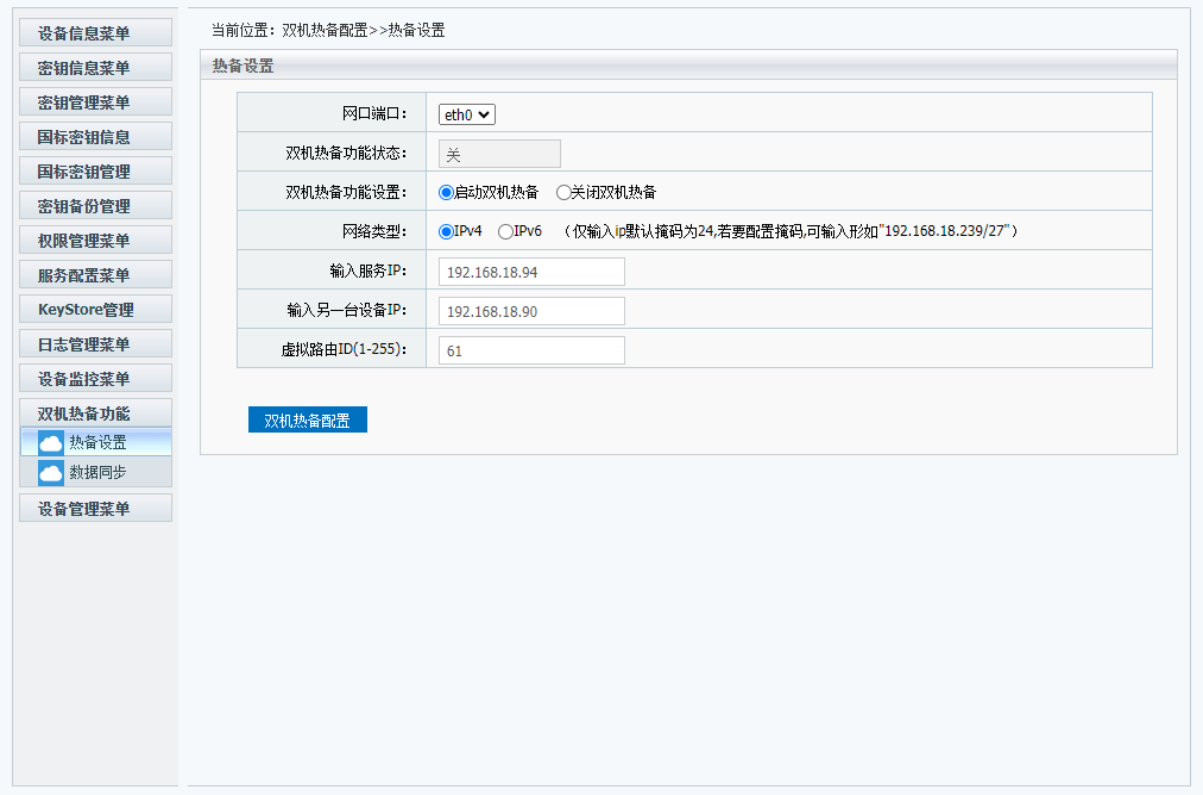

图 62

另一台加密机也需要进行类似的配置。

开启双机热备功能后，先启动的加密机会将自己的IP设置为双机热备服务设备的IP；后启动的加密机则将自己的IP设置为从机IP 即 从服务设备的IP。如图63所示。

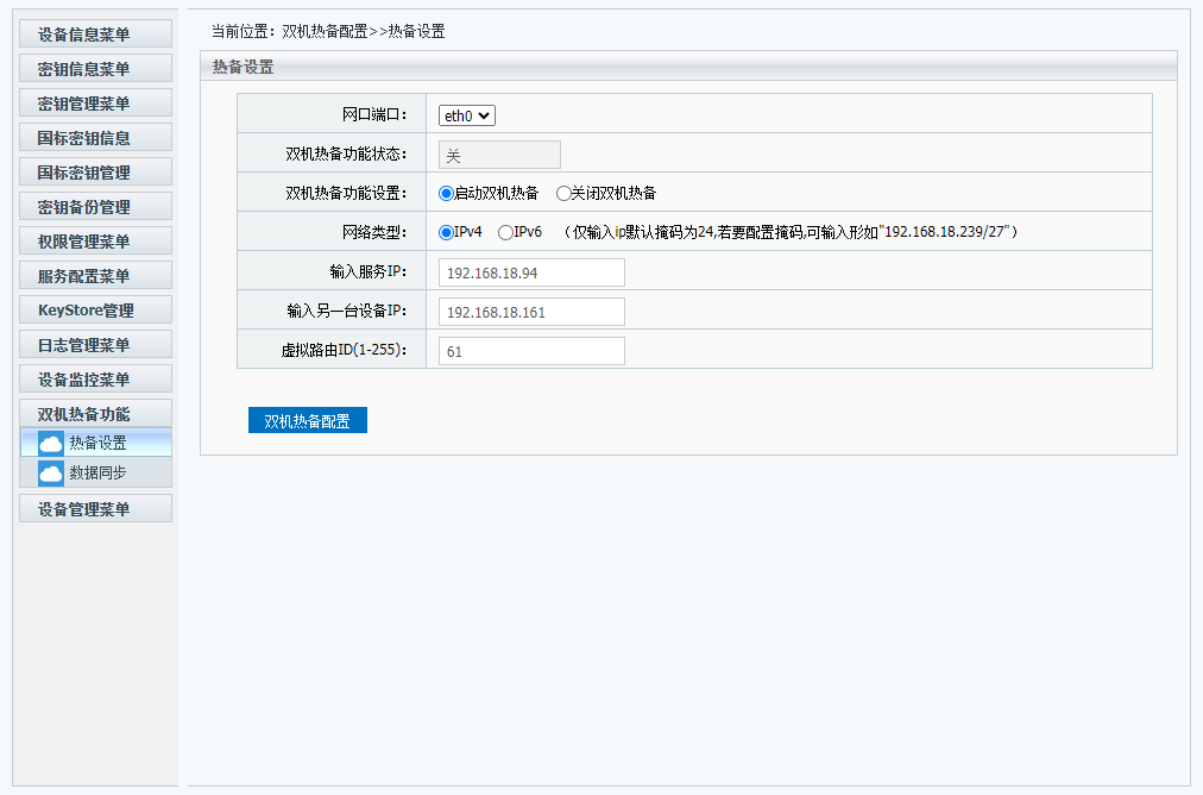

图 63

注意：1)、虚拟路由ID，如果加密机A和B共同完成双机热备，那么两台加密机配置的虚拟路由ID应该一致，如果同一网络中，有多个主备组，那么他们的虚拟路由ID不能重复

2) 、服务设备IP 要是一个非加密机A 和加密机B的局域网内没有使用的第三方IP

（二）、关闭双机热备功能：

首先，点击选中 “关闭双机 热备”来关闭双机热备功能；然后点击 “双击热备配置” 按钮 ，来保存配置信息。重启加密机服务器后，双机热备的设置才能生效。

关闭双击设备功能后，加密机服务器会配置 为自己原本的IP。

3.8.2 服务器密码机数据同步

单击左侧菜单栏“双机热备”按钮，并单击“数据同步”按钮，如图64。

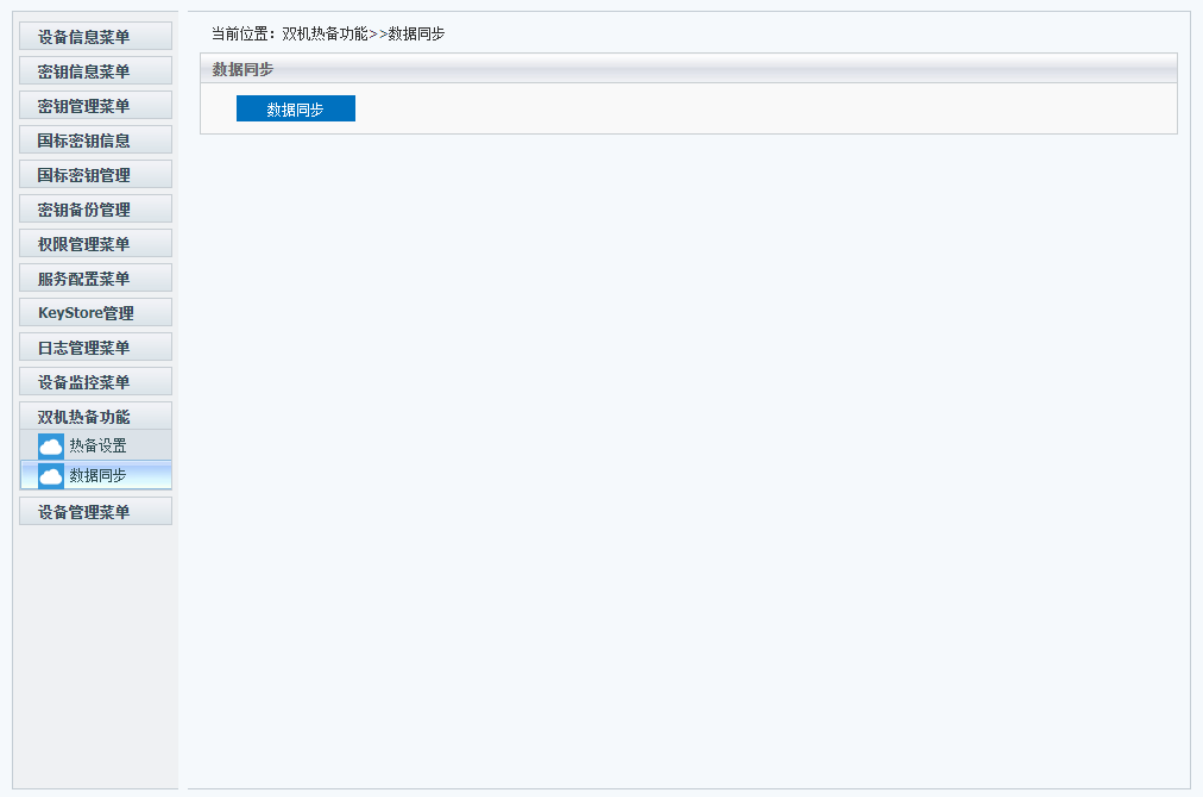

图 64

3.9 服务器密码机初始化

在设备出厂后，用户进行操作之前，需要进行设备初始化操作。连接后输入用户名密码：默认用户名：admin，密码：admin，首先将服务器密码机ETH0网口接入网络，服务器密码机默认连接IP地址是https://192.168.18.239。连接后输入用户名密码，如图65：

图 65

输入用户名、密码后，点击登陆，进入管理界面如图66：

图 66

首先鼠标单击左侧菜单栏“设备管理”，再单击“设备初始化”按钮，进入初始化操作界面。如图67所示。

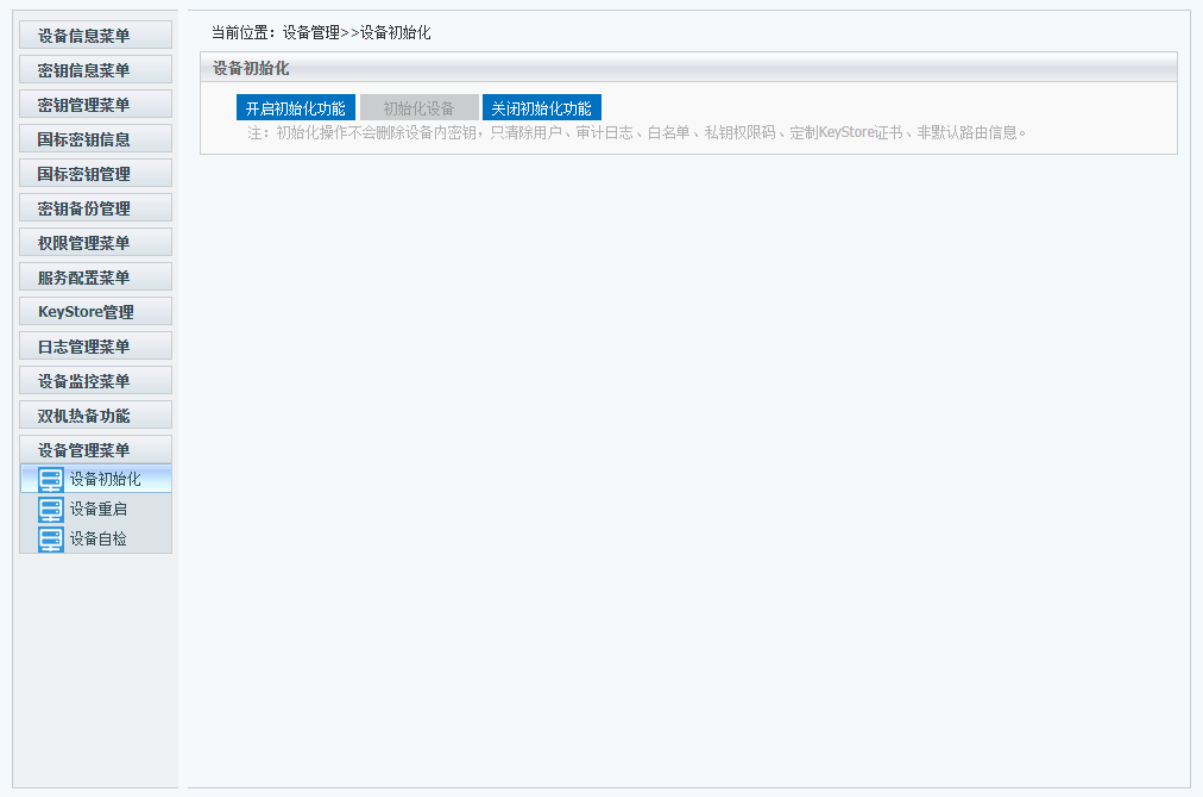

图 67

鼠标单击中间按钮“开启初始化功能”，弹框提示“确定开启初始化功能”，选择确定之后，开启初始化成功后提示。然后，鼠标单击 “初始化设备”按钮，如图68、69所示。

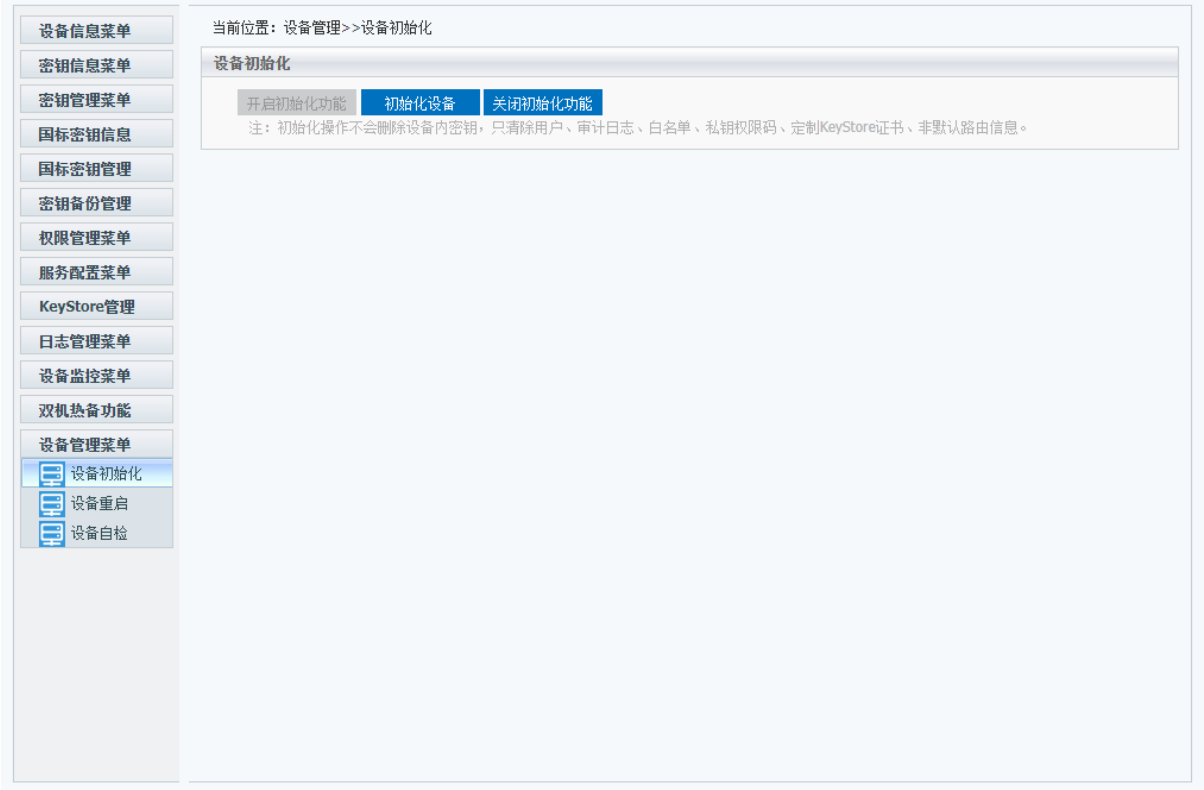

图 68

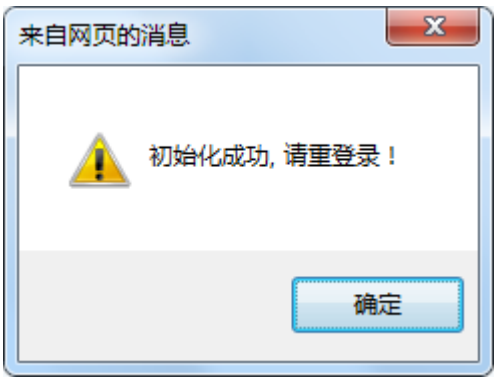

图 69

点击确定后，页面回退到登录界面，需要重新输入账号：admin，口令：admin，重新登录进入加密机管理页面。注：初始化操作不会删除设备内密钥，只清除管理员、审计日志、白名单、定制KeyStore证书。

到此，初始化操作已经完成，需要重新启动加密机来达到初始化目的。单击左侧菜单栏“设备重启”栏，选择“服务器重启”页面，如图70。

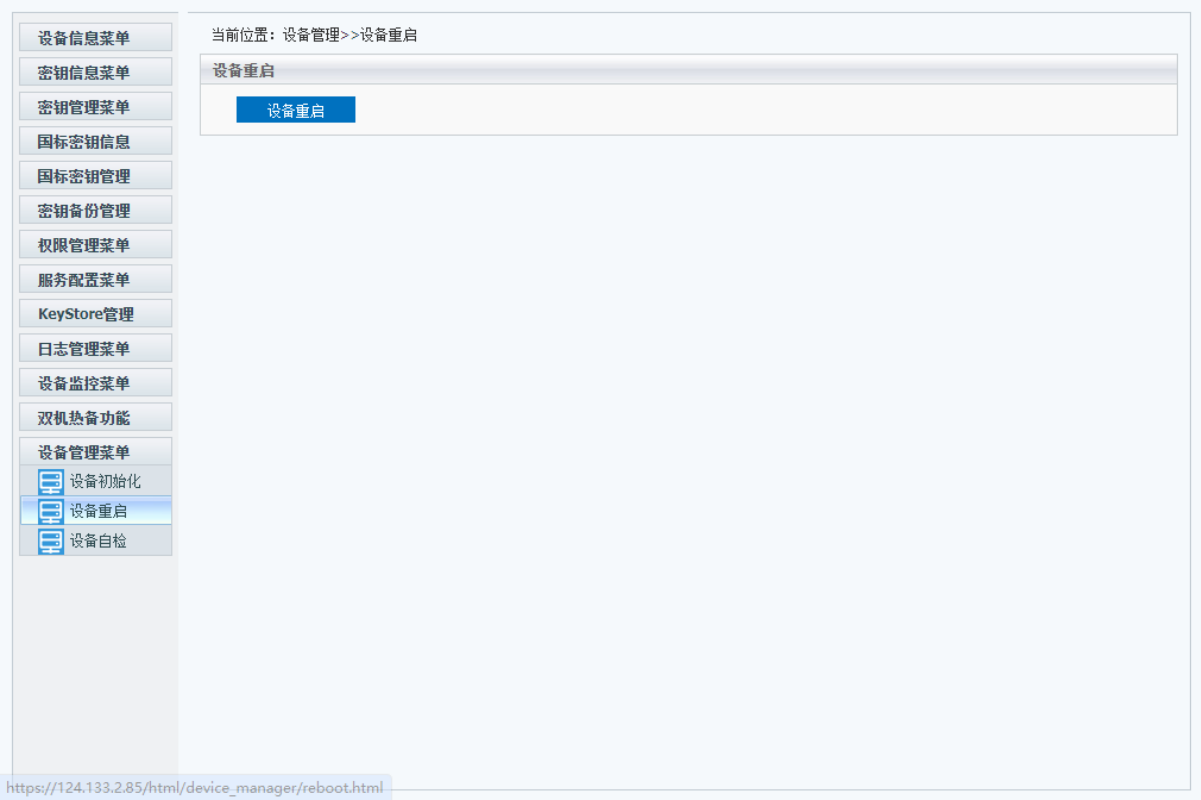

图 70

等待机器重启完毕，可再次登陆web配置界面进行其他配置。登陆页面会变成如图71。

图 71

用户名变为已添加管理员的序列号，将任意管理员插入配置终端的usb接口中，并在用户名处选择插入key的对应序列号，密码处输入对应的密码，默认是“12345678”，点击登陆后可以进入配置页面。否则不插入管理员无法进入配置页面。

4 产品常见错误分析及解决方法

4.1 服务器密码机配置管理连接不上

首先确认服务器密码机的ip地址输入正确。可通过ping命令来确定网络是否连接正常，有如下原因可导致网络连接不上：

- ✧ 客户端ip地址和服务器密码机连接网口对应的ip地址不在同一网段内。
- ✧ 服务器密码机配置了多个在同一网段的ip地址（服务器密码机的每个网口必须设置不同ip网段）。
- ✧ 设置了新的ip地址后，没有重新启动服务器密码机，而导致ip没有修改。

4.2 服务器密码机服务连接不上

当服务器密码机配置管理可以连接，而服务无法连接时，可能有如下原因：

- ✧ 客户端配置文件没有放到系统目录下。
- ✧ 客户端配置文件中ip没有设置成连接服务器密码机的ip地址。
- ✧ 客户端配置文件的最后一行不是空行。
- ✧ 服务端口号8012被屏蔽。

4.3 服务器密码机服务报错

在进行密钥生成、删除，备份、恢复操作时，需要管理员权限，否则报错。