

时间戳服务器用户手册

目录

1. 产品概述	4
1.1. 产品简介	4
1.2. 产品功能	4
1.3. 适用对象	5
2. 快速使用指南	6
2.1. 安装时间戳服务器	6
2.2. 产品部署	6
2.3. 时间戳服务器初始化	18
2.3.1. 初始化系统超级管理员	18
2.3.2. 初始化系统审计管理员	18
2.3.3. 下载安装托盘程序	19
2.3.4. 登录时间戳服务器	19
3. 时间戳服务器功能	18
3.1. 系统超级管理员	21
3.1.1. 用户管理	21
3.2. 系统管理员	22
3.2.1. 设备导航	22
3.2.2. 服务配置	23
3.2.3. 设备授权	23
3.2.4. 网络管理	24
3.2.5. 时间配置	27
3.2.6. 设备状态	29
3.2.7. 设备运维	30
3.2.8. 设备重置	31
3.2.9. 设备升级	32
3.3. 审计管理员	32
3.3.1. 日志管理	32
3.4. 安全管理员	34
3.4.1. 设备导航	34
3.4.2. 密码卡用户管理	35
3.4.3. 密钥管理	36
3.4.4. 证书链管理	43
3.4.5. 时间戳管理	44

3.4.6. HTTP 鉴权管理	48
3.4.7. 服务配置	49
3.4.8. 白名单管理	50
3.4.9. 设备状态	51
3.4.10. 系统备份恢复	51

1. 产品概述

1.1. 产品简介

时间戳服务器（以下简称“时间戳服务器”）是由我司自主研发的高性能密码设备，能够为各类业务系统提供高性能的、多任务并行处理的密码运算，支持 SM1、SM2、SM3、SM4 等多种国产密码算法，具有证书管理、密钥安全存储、设备管理、访问控制、高速密码运算、真随机数生成、日志审计和设备自检等功能。可以满足应用系统数据的签名/验证、加密/解密的要求，保证传输信息的机密性、完整性和有效性，同时提供安全、完善的密钥管理机制，自身具备较强的安全防护能力。

应用系统通过调用时间戳服务器提供的标准 API 函数来使用时间戳服务器的服务，时间戳服务器 API 与时间戳服务器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时间戳服务器所提供的安全功能。时间戳服务器 API 接口符合《GM/T 0029-2014 时间戳服务器技术规范》接口规范，API 支持主流操作系统，具有很强的环境适用性，能够平滑接入各种系统平台，满足大多数应用系统的要求。支持通过 WEB 方式对设备进行管理和证书配置，易用性高、管理方便。在应用系统安全方面具有广泛的应用前景。

1.2. 产品功能

- ✓ **数字时间戳：**实现对各类电子数据的数字签名功能，支持多种数字签名格式，支持文件时间戳功能；
- ✓ **时间戳格式：**支持 PKCS#1、PKCS#7 Attach、PKCS#7 Detach、XML 等格式的数据签名、签名验证功能；
- ✓ **数据加密解密功能：**实现对各类电子数据的数据加密解密功能，支持非对称加密、对称加密；
- ✓ **数字信封功能：**支持基于 RSA、SM2 密码算法的数字信封功能，支持 PKCS#7 标准各种格式的数字信封封装和解封；
- ✓ **证书验证方式：**支持 CA、CRL、OCSP 等多种方式证书有效性验证；
- ✓ **用户证书支持：**支持符合 X.509 标准的证书，支持证书链功能；
- ✓ **多 CA 证书支持：**支持配置多个 CA 或者多级 CA，可同时配置多条证书链；

- ✓ **证书解析功能:**提供用户证书解析功能,获取证书中的任意主题信息以及扩展项信息;
- ✓ **时间同步功能:**支持通过配置的 NTP 时间源定时自动同步系统时间,确保签名、验证证书等业务的有效性;
- ✓ **B/S 架构管理:**支持通过 Web 方式进行系统管理、密钥和证书管理、服务配置管理、日志审计等;
- ✓ **日志管理功能:**系统自行记录日志,也可以将日志以 syslog 的方式发送到指定服务器,并提供日志审计功能;
- ✓ **系统备份及恢复:**支持系统信息的备份和恢复功能,保证了安全应用系统的安全性和可靠性。

1.3. 适用对象

本手册适用于时间戳服务器的用户操作指导。

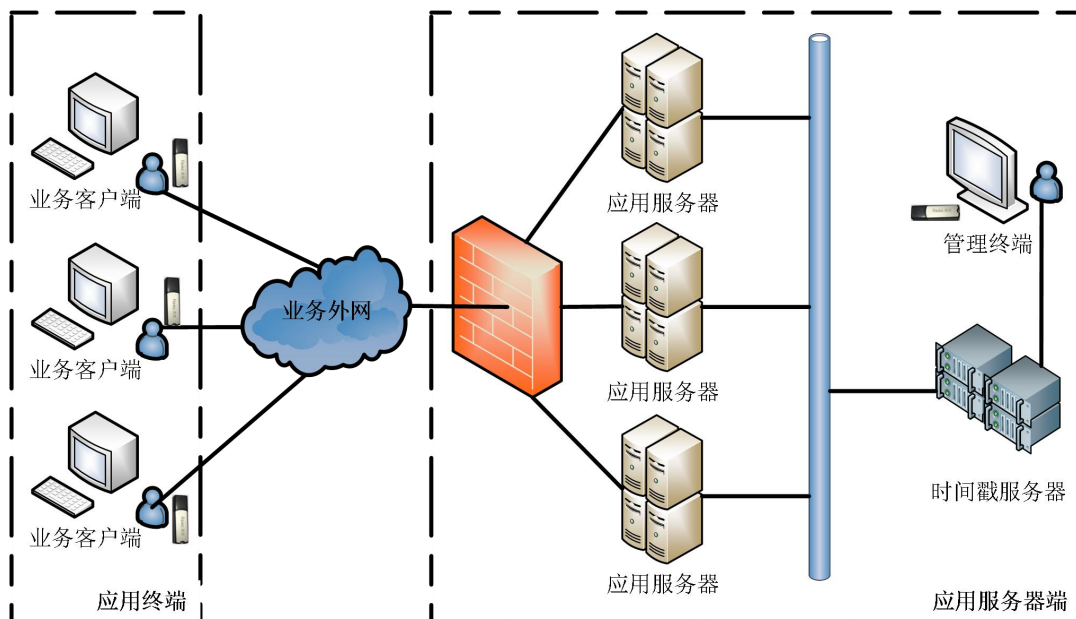
2. 快速使用指南

2.1. 安装时间戳服务器

- (1) 打开包装，对照“装机清单”检查配件是否齐全；
- (2) 取出时间戳服务器主机，使用包装内的电源线连接电源；
- (3) 打开电源开关，启动时间戳服务器主机。
- (4) 服务器一共四个网口，分别是 eth0: 192.168.5.10、eth1: 192.168.6.10、eth2: 192.168.7.10、eth3: 192.168.8.10。eth0-eth2 是服务口，eth3 是管理口。

2.2. 产品部署

时间戳服务器的网络部署图如下图所示。



2.3. 时间戳服务器使用部署

2.3.1. 网络配置

打开电源开关，启动主机进行网络配置（默认为 eth0: 192.168.5.10
eth1: 192.168.6.10 eth2: 192.168.7.10 eth3: 192.168.8.10

注：信创的设备为两个网口（默认为 eth0: 192.168.5.10 eth1:
192.168.6.10)

将电脑与服务器密码机的管理口（eth3）数字最大口直连，需使用**非 iel1 内核浏览器**登录管理口（192.168.8.10）在浏览器中直接输入：
192.168.8.10，回车则显示设备登录界面。管理员有两种登录方式分别是
密码登录和 UKey 登录。

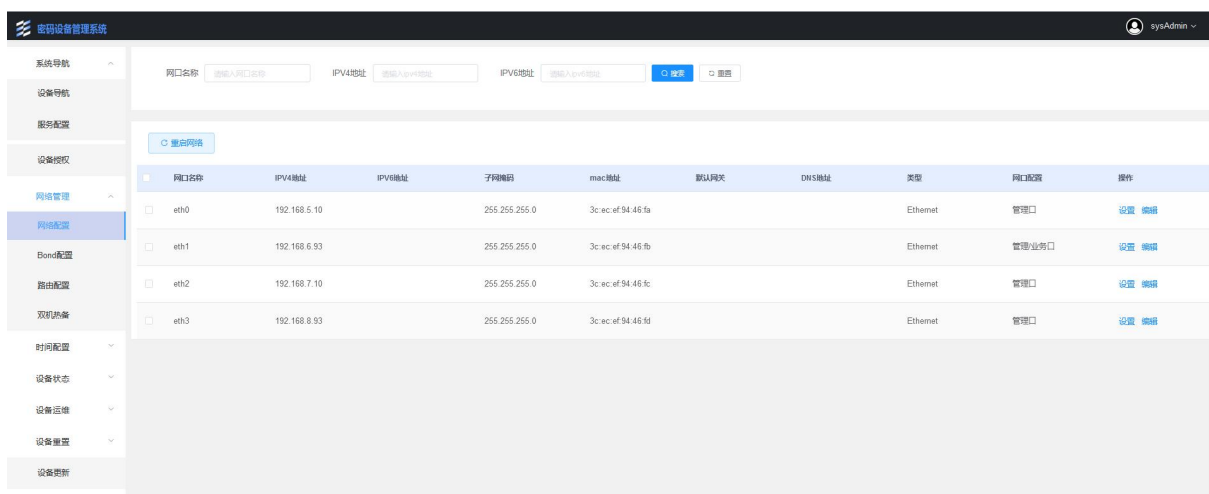
密码登录：点击【密码登录】，填写账号、密码、图片验证码，然后
点击【登录】按钮，系统验证通过，进入服务器密码机。



UKey 登录：如果没安装插件，点击下载登陆插件。安装完之后启动，每次登录需要启动插件程序。点击【UKey 登录】，插入 Web 页面 Ukey，填写 PIN、密码，然后点击【登录】按钮，系统验证通过，进入服务器密码机。

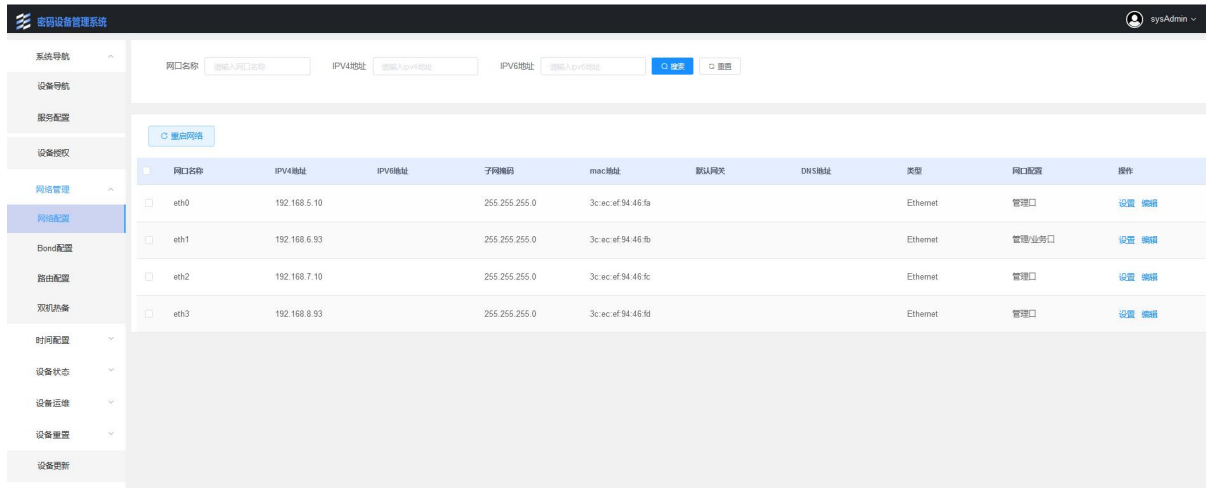


将系统管理员的 key 插入电脑的 usb 接口，登录系统管理员修改所需要的 ip，配置好后点击保存后重启网络，改好之后电脑直连修改的 ip 对应网口 ping 一下确保配置的 ip 段能够 ping 通。（登录 web 管理界面的口令：12345678）



业务 IP 配置：

根据客户提供的业务 IP 地址进行配置，需设置 IP 地址、子网掩码、默认网关等信息，配置完成后会自动重启。



根据客户需求是否开启双机热备模式，如开启需填写对应信息，需分配主机 IP 地址，备机 IP 地址，以及虚拟 IP 地址等三个 IP 地址，注意填写的对应地址。

新增双机热备
✕

* 名称

* 虚拟地址

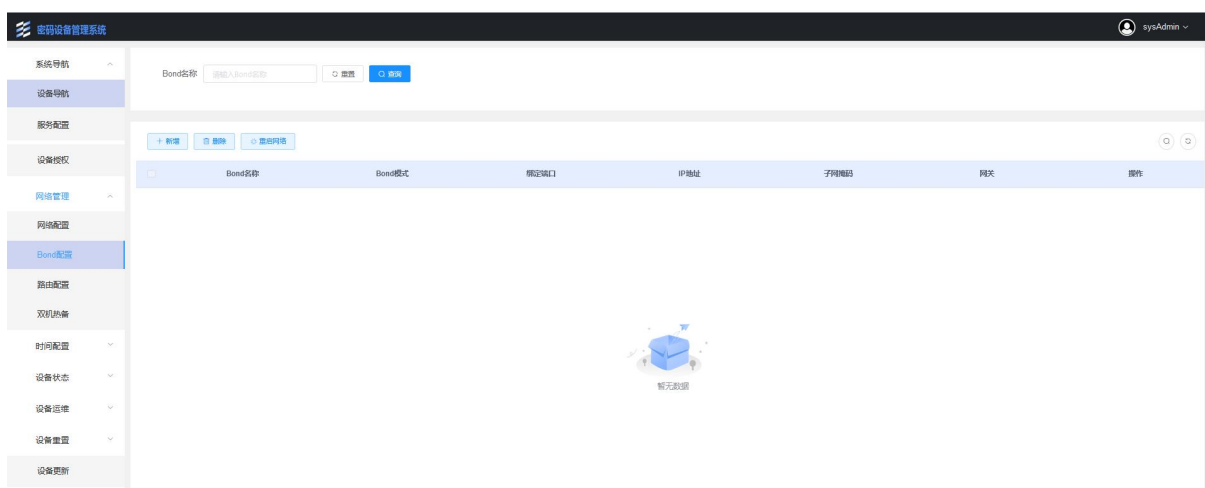
* 备机地址

* 虚拟组id

* 绑定模式

* 绑定网口 eth0 eth1

根据客户网络需要开启 bond 配置，网络主备模式需占用服务器两个网络接口，填写时注意网络接口的名称不要选错，以及对应 IP 地址、子网掩码、网关等信息，配置完成需要重启网络生效。



2.3.2. 密钥配置

设备出厂时默认生成 SM2 密钥（1-20）、RSA2048（1-20）、长度

为 16 的对称密钥（1-20），也可以直接使用，跳过该步骤。

根据客户需求数量生成密钥，其中密钥标签为密钥数量，根据实际需求数量填写，密钥用途选择签名和加密，根据密钥类型选择密钥模长。

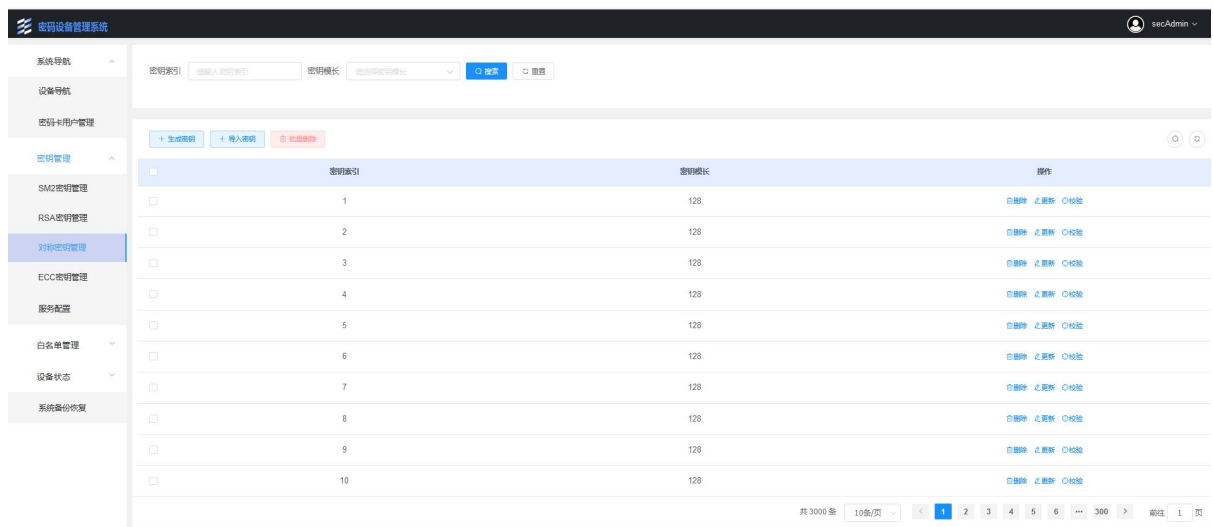
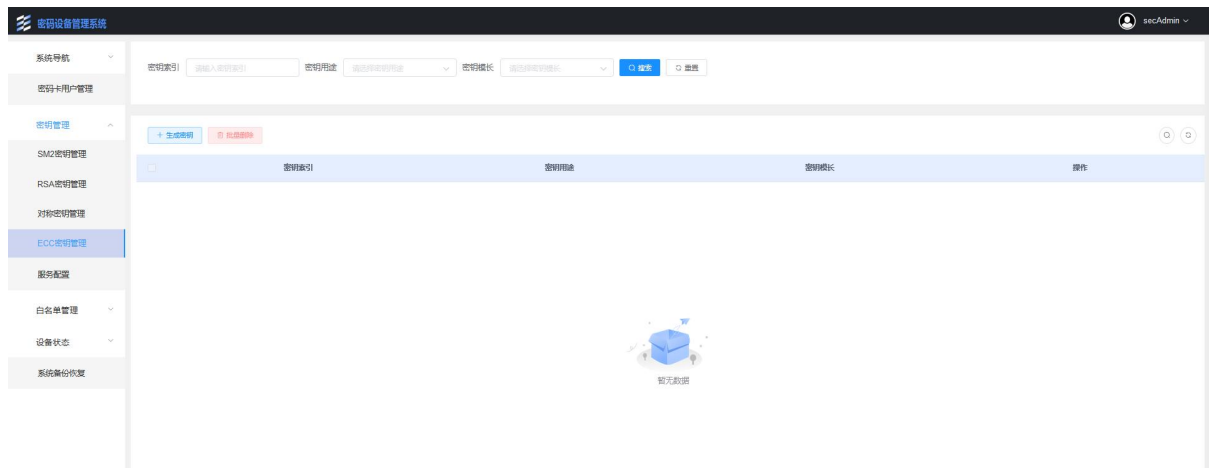
密钥生成如下图所示：

The screenshot shows the '密钥设备管理系统' (Key Management System) interface. The left sidebar contains navigation options like '系统导航', '设备导航', '密钥卡用户管理', '密钥管理', 'SM2密钥管理', 'RSA密钥管理', '对称密钥管理', 'ECC密钥管理', '服务器配置', '白名单管理', '设备状态', and '系统备份恢复'. The main area displays a table of generated keys with the following columns: '密钥索引' (Key Index), '密钥用途' (Key Purpose), '密钥模长' (Key Length), and '操作' (Action). The table shows 10 rows of keys, all with a length of 2048 bits. The '操作' column includes links for '删除' (Delete), '更新' (Update), and '导出密钥' (Export Key). At the bottom, it indicates '共 400 条' (Total 400 items) and '10条/页' (10 items per page).

密钥索引	密钥用途	密钥模长	操作
1	签名密钥	2048	删除 更新 导出密钥
1	加密密钥	2048	删除 更新
2	签名密钥	2048	删除 更新 导出密钥
2	加密密钥	2048	删除 更新
3	签名密钥	2048	删除 更新 导出密钥
3	加密密钥	2048	删除 更新
4	签名密钥	2048	删除 更新 导出密钥
4	加密密钥	2048	删除 更新
5	签名密钥	2048	删除 更新 导出密钥
5	加密密钥	2048	删除 更新

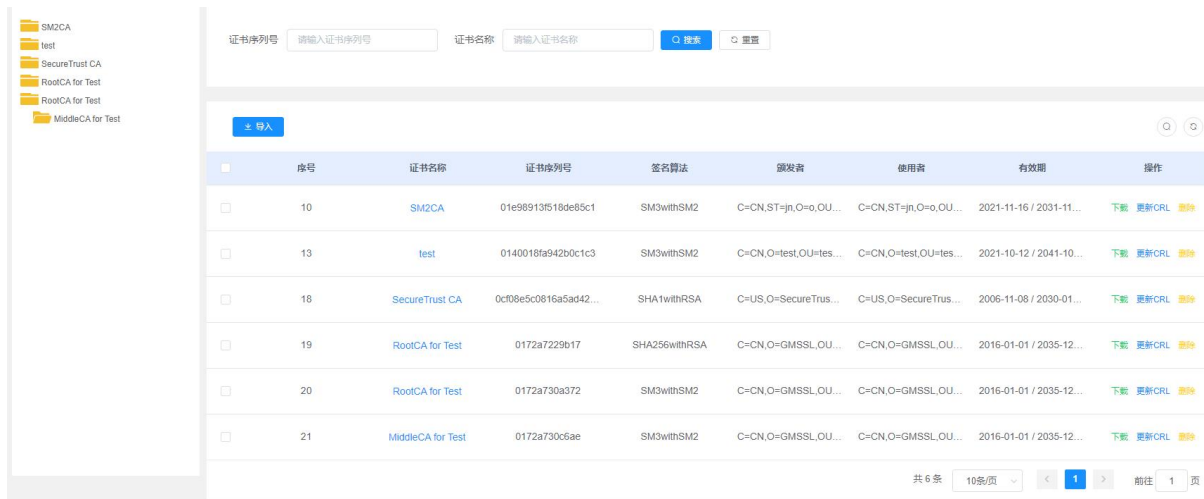
The screenshot shows the '密钥设备管理系统' (Key Management System) interface. The left sidebar contains navigation options like '系统导航', '设备导航', '密钥卡用户管理', '密钥管理', 'SM2密钥管理', 'RSA密钥管理', '对称密钥管理', 'ECC密钥管理', '服务器配置', '白名单管理', '设备状态', and '系统备份恢复'. The main area displays a table of generated keys with the following columns: '密钥索引' (Key Index), '密钥用途' (Key Purpose), '密钥模长' (Key Length), and '操作' (Action). The table shows 10 rows of keys, all with a length of 256 bits. The '操作' column includes links for '删除' (Delete), '更新' (Update), '导出密钥' (Export Key), and '导出公钥' (Export Public Key). At the bottom, it indicates '共 5000 条' (Total 5000 items) and '10条/页' (10 items per page).

密钥索引	密钥用途	密钥模长	操作
1	签名密钥	256	删除 更新 导出密钥 导出公钥
1	加密密钥	256	删除 更新 导出公钥
2	签名密钥	256	删除 更新 导出密钥 导出公钥
2	加密密钥	256	删除 更新 导出公钥
3	签名密钥	256	删除 更新 导出密钥 导出公钥
3	加密密钥	256	删除 更新 导出公钥
4	签名密钥	256	删除 更新 导出密钥 导出公钥
4	加密密钥	256	删除 更新 导出公钥
5	签名密钥	256	删除 更新 导出密钥 导出公钥
5	加密密钥	256	删除 更新 导出公钥



2.3.3.根证书管理

添加根证书：添加 ROOT 证书或证书链，受信任证书颁发机构章节(根证书本项目使用的 CA 提供)。

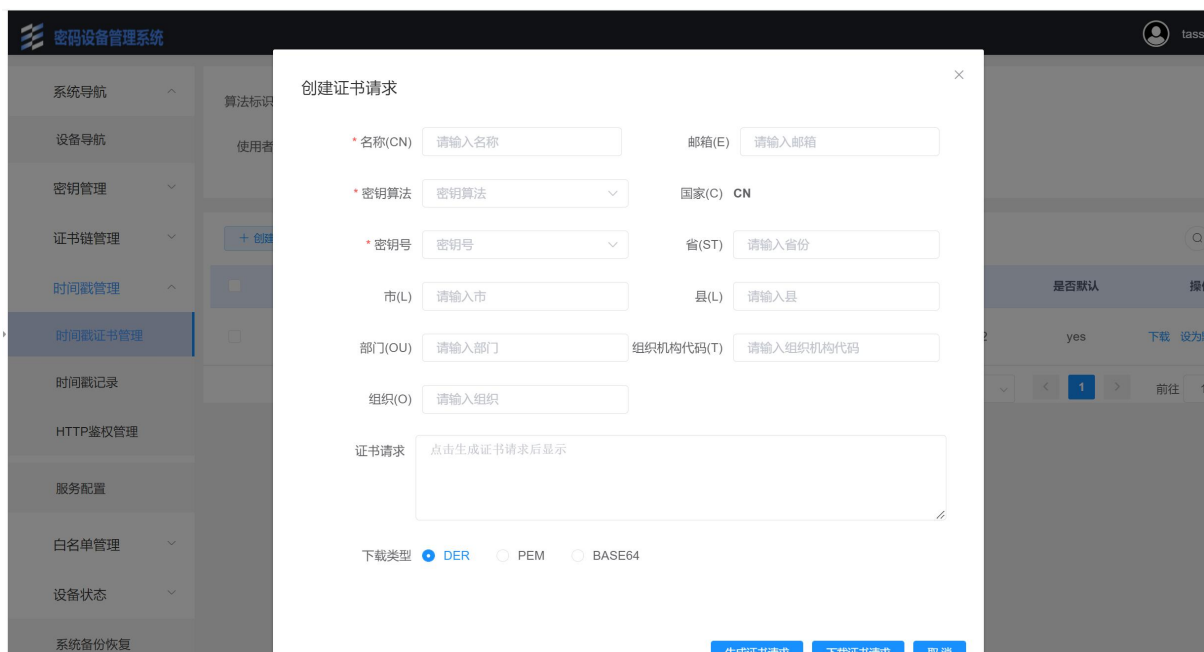


序号	证书名称	证书序列号	签名算法	颁发者	使用者	有效期	操作
10	SM2CA	01e98913f518de65c1	SM3withSM2	C=CN,ST=jin,O=o,OU...	C=CN,ST=jin,O=o,OU...	2021-11-16 / 2031-11-...	下载 更新CRL 删除
13	test	0140018fa942b0c1c3	SM3withSM2	C=CN,O=test,OU=tes...	C=CN,O=test,OU=tes...	2021-10-12 / 2041-10-...	下载 更新CRL 删除
18	SecureTrust CA	0cf08e5c0816a5ad42...	SHA1withRSA	C=US,O=SecureTrus...	C=US,O=SecureTrus...	2006-11-08 / 2030-01-...	下载 更新CRL 删除
19	RootCA for Test	0172a7229b17	SHA256withRSA	C=CN,O=GMSSSL,OU...	C=CN,O=GMSSSL,OU...	2016-01-01 / 2035-12-...	下载 更新CRL 删除
20	RootCA for Test	0172a730a372	SM3withSM2	C=CN,O=GMSSSL,OU...	C=CN,O=GMSSSL,OU...	2016-01-01 / 2035-12-...	下载 更新CRL 删除
21	MiddleCA for Test	0172a730c6ae	SM3withSM2	C=CN,O=GMSSSL,OU...	C=CN,O=GMSSSL,OU...	2016-01-01 / 2035-12-...	下载 更新CRL 删除

2.3.4.用户证书管理

1) 申请 P10

申请时间戳证书，名称以密钥对应号命名，证书导入时便于区分，客户信息按照实际填写，选择对应密钥号，先提交请求生成 PKCS10 内容，在点击下载保存。将导出的 P10 请求文件发给第三方 CA 机构，CA 机构会传回对应的证书)



创建证书请求

* 名称(CN) 邮箱(E)

* 密钥算法 国家(C)

* 密钥号 省(ST)

市(L) 县(L)

部门(OU) 组织机构代码(T)

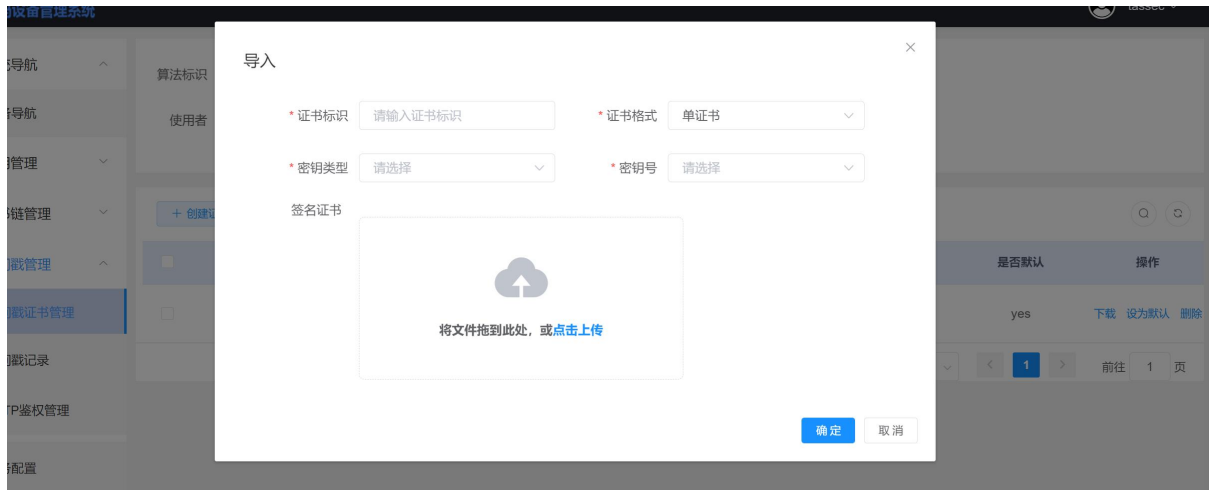
组织(O)

证书请求

下载类型 DER PEM BASE64

2) 导入时间戳证书和设置默认证书

导入证书后，需要设备为默认证书才能生效



证书标识	证书序号	对应密钥	使用者	颁发者	算法标识	是否默认	操作
<input type="checkbox"/>	SM2_1	01886c6fe68c	1号	C=CN,O=,CN=test,C	C=CN,O=GMSS...	SM3withSM2	yes 下载 设为默认 删除

共 1 条 10条/页 < 1 > 前往 1 页

2.3.5. 备份恢复

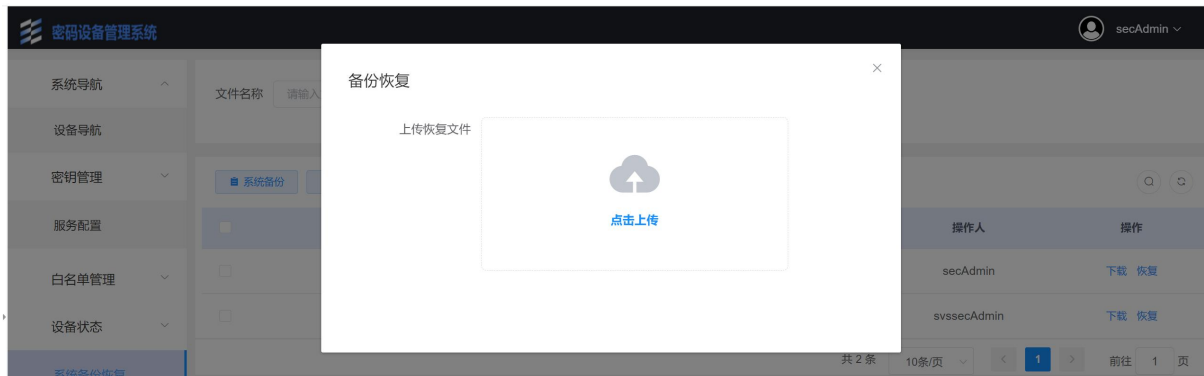
(1) 点击“系统备份”，生成之后如下图，需要下载就点击下载。

文件名称	备份时间	恢复时间	操作人	操作
<input type="checkbox"/>	crypto20230531102652.tar.gz	2023-05-31 10:26:52	secAdmin	下载 恢复
<input type="checkbox"/>	crypto20230530114047.tar.gz	2023-05-30 11:40:47	svssecAdmin	下载 恢复

共 2 条 10条/页 < 1 > 前往 1 页

(2) 备份恢复：如密钥丢失或错误，需恢复备份文件来修复。如有两台密

码机做双机热备，也需要在备用机恢复主机的备份来完成主备模式设置。



2.3.6. 验证配置正确性

(1) 利用系统内置 ping 工具，首先 ping 网关，再 ping 网络中的其他密码设备的 IP 地址，查看网络连通情况，保证网络连通。

(2) 使用 telnet 工具检测“IP+端口”，查看连接状态是否正常。

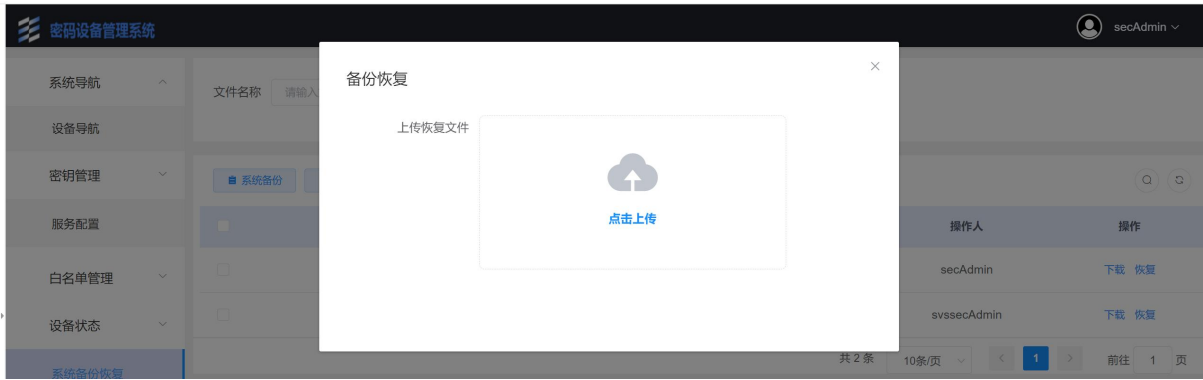
2.3.7. 集群配置

注：多台相同服务器根据业务需求考虑做不做，单台设备忽略该章节

(1) 网络配置：根据需求配置 ip 地址（系统管理员）。

(2) 密钥恢复：恢复保存设备备份数据到本机系统恢复。

其他设备配置：其他设备重复本章节流程。



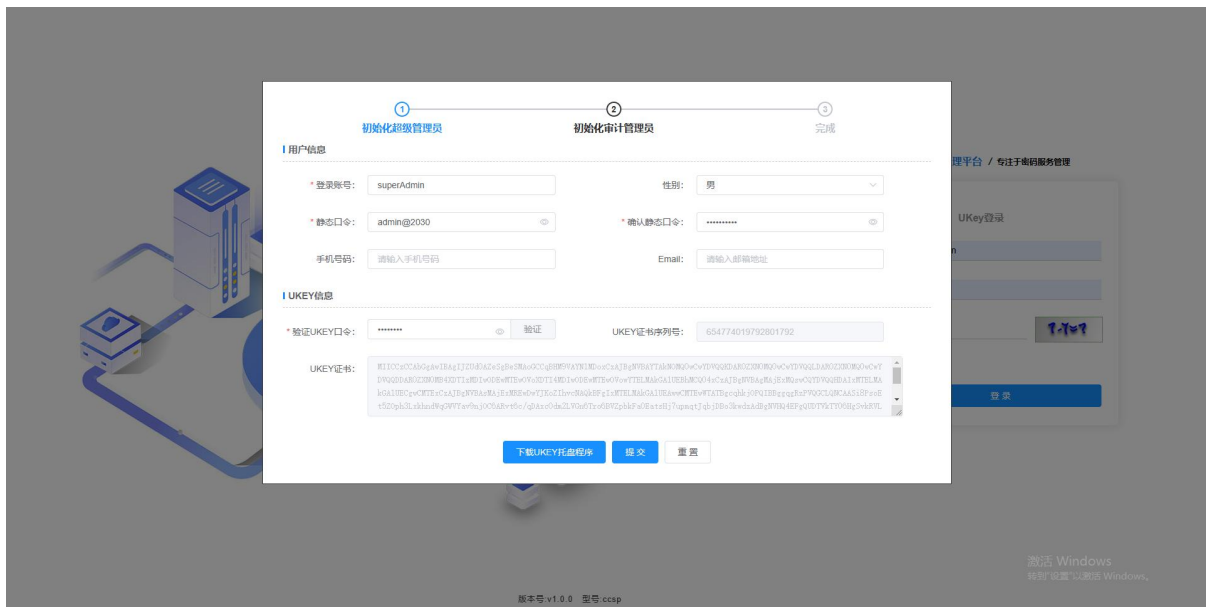
3. 时间戳服务器功能

时间戳服务器默认具有超级管理员、系统管理员、审计管理员、安全管理员 4 个角色。注意用户可再次添加新角色，然后再赋予相应的权限。

3.1. 时间戳服务器初始化

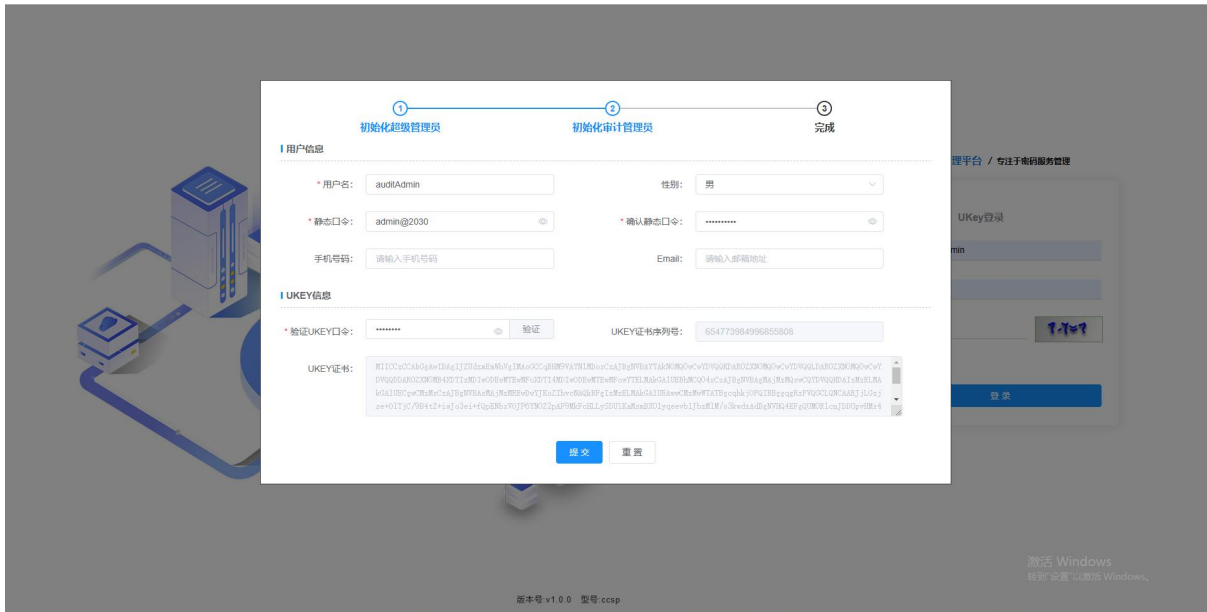
3.1.1. 初始化系统超级管理员

首先初始化系统超级管理员，将超级管理员 UKey 插入计算机的 USB 接口，按照提示输入两次口令，点击“初始化超级管理员”，初始化成功后自动跳转到下一个页面。



3.1.2. 初始化系统审计管理员

初始化完系统的超级管理员之后，会自动跳转到初始化系统审计管理员，初始化方式与初始化系统超级管理员相同，初始化完毕后，自动跳转登陆界面。



3.1.3. 下载安装 UKEY 插件程序

登录页面选择 Ukey 登录，点击右下角【下载 UKEY 插件程序】，即可在浏览器完成下载。下载完成后，解压压缩包，点击安装程序，根据提示安装即可。



3.1.4. 登录时间戳服务器

管理员有两种登录方式分别是密码登录和 UKey 登录。

密码登录：点击【密码登录】，填写账号、密码、图片验证码，然后点击【登录】按钮，系统验证通过，进入密钥管理平台。如下图所示：



The screenshot shows a login form with the following elements:

- Header: 密码登录 | UKey登录
- Username field: user
- Password field: masked with dots
- Image verification code field: 4, with a sample image showing the code 7-3-7
- Remember password checkbox: checked, labeled 记住密码
- Login button: 登录

UKey 登录：点击【UKey 登录】，插入 Web 页面 Ukey，填写 PIN、密码，然后点击【登录】按钮，系统验证通过，进入密钥管理平台，如下图所示：



3.2. 系统超级管理员

3.2.1. 用户管理

管理员管理包括新建管理员、管理员列表。

3.2.1.1. 新建用户

点击【新增】。管理员类型可以选择系统管理员、系统安全管理员，（注：这里新增管理员的时候，已经插在计算机上的超级管理员的 key 不动，直接将新的 key 插到计算机上即可），插入新的 key，选择要生成的管理员类型，输入口令，点击“提交”按钮，管理员生成成功。

添加用户
×

用户信息

* 认证模式:

* 静态口令:

手机号码:

归属部门:

* 用户名:

* 确认静态口令:

邮箱:

* 角色:

3.2.1.2. 用户列表

可以在管理员列表中查看生成的管理员，如下图所示。内容包括管理员的登录名、管理员类型、管理员状态。处于正常状态的管理员可以登录，处于锁定状态的管理员不可以登录。对于管理员 key 丢失的情况，我们可以对丢失的 key 的管理员进行锁定操作，以提高系统使用的安全性。

用户编号	用户名称	用户昵称	部门	手机号码	状态	创建时间	操作
101	supAdmin	超级管理员	若依科技		<input checked="" type="checkbox"/>	2023-01-04 11:01:18	修改 删除 更多
102	audAdmin	审计管理员	若依科技		<input checked="" type="checkbox"/>	2023-01-04 11:01:44	修改 删除 更多
103	secAdmin	安全管理员-HSM	若依科技		<input checked="" type="checkbox"/>	2023-01-04 11:02:29	修改 删除 更多
104	sysAdmin	系统管理员	若依科技		<input checked="" type="checkbox"/>	2023-01-04 11:02:55	修改 删除 更多
105	secAdmin2	安全管理员-SVS			<input checked="" type="checkbox"/>	2023-01-04 15:56:04	修改 删除 更多
106	secAdmin3	安全管理员-TSA			<input checked="" type="checkbox"/>	2023-01-04 16:38:14	修改 删除 更多
107	audAdmin_vpn	审计管理员-VPN			<input checked="" type="checkbox"/>	2023-01-04 17:04:46	修改 删除 更多
108	sysAdmin_vpn	系统管理员-VPN			<input checked="" type="checkbox"/>	2023-01-04 17:59:43	修改 删除 更多
109	secAdmin_ssl	安全管理员-SSL			<input checked="" type="checkbox"/>	2023-01-05 10:17:38	修改 删除 更多
110	secAdmin_ipsec	安全管理员-IPSec			<input checked="" type="checkbox"/>	2023-01-05 11:12:55	修改 删除 更多

3.3. 系统管理员

3.3.1. 设备导航

可以进行系统配置的快捷跳转，以便更方便的进行操作。



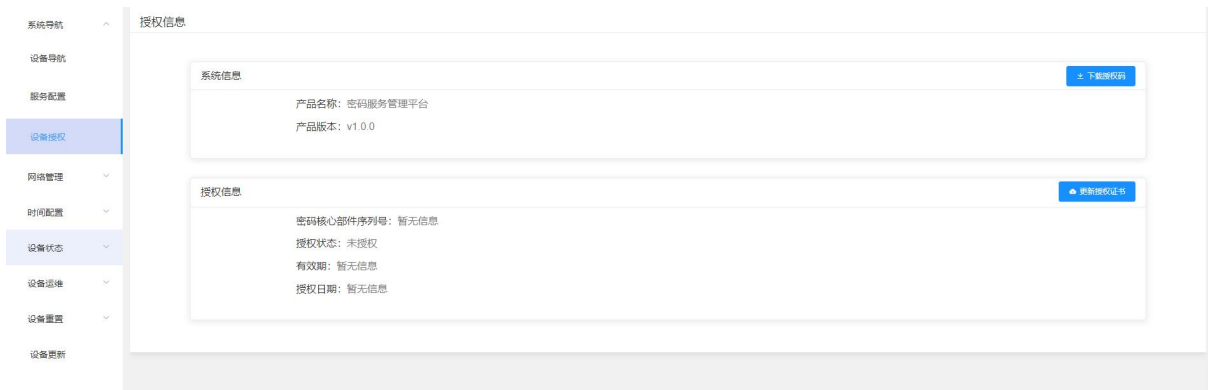
3.3.2. 服务配置

服务配置主要修改服务配置信息，包括服务器密码机端口最大数量、服务器密码机端口配置数量、服务器密码机端口，输入完信息后，点击【确认】，点击【重启服务】，使修改的配置生效。



3.3.3. 设备授权

可以查看授权信息，下载授权码和更新授权证书。

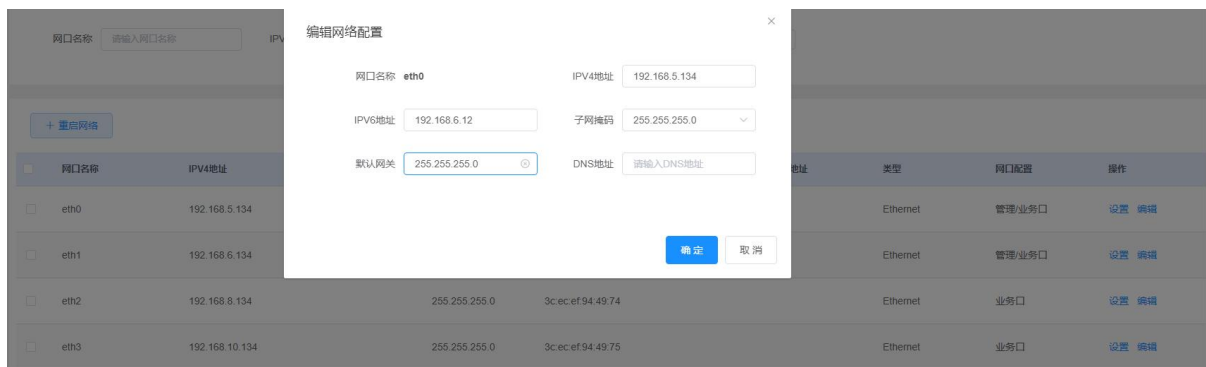


3.3.4. 网络管理

3.3.4.1. 网络配置

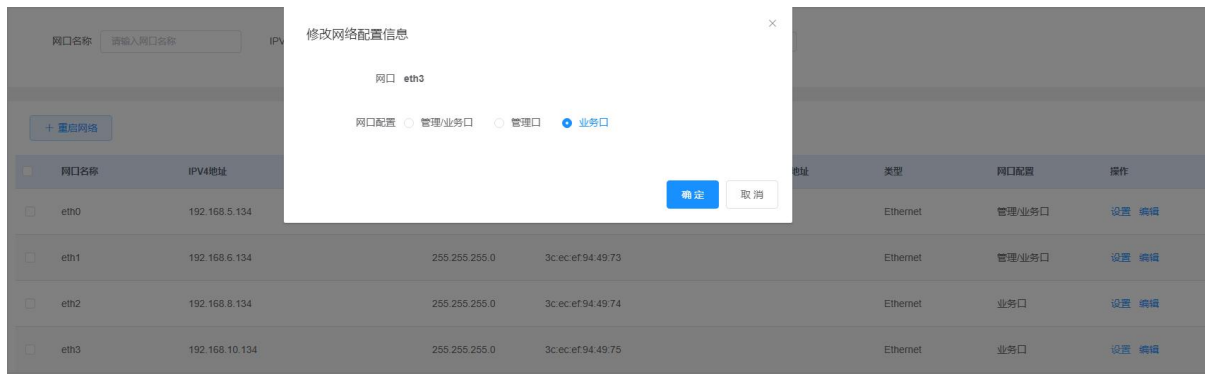
3.3.4.1.1. 编辑

点击【编辑】，在弹出的对话框中可修改 IPV4 地址、IPV6 地址、子网掩码、默认网关、DNS 地址，然后【确认】完成编辑。注意每个的格式都要填写正确。点击重启后生效。点击重启后生效。



3.3.4.1.2. 设置网口类型

点击【设置】，在弹出的对话框中可选择管理口、业务口，然后【确认】完成设置。点击重启后生效。点击重启后生效。



3.3.4.2. Bond 配置

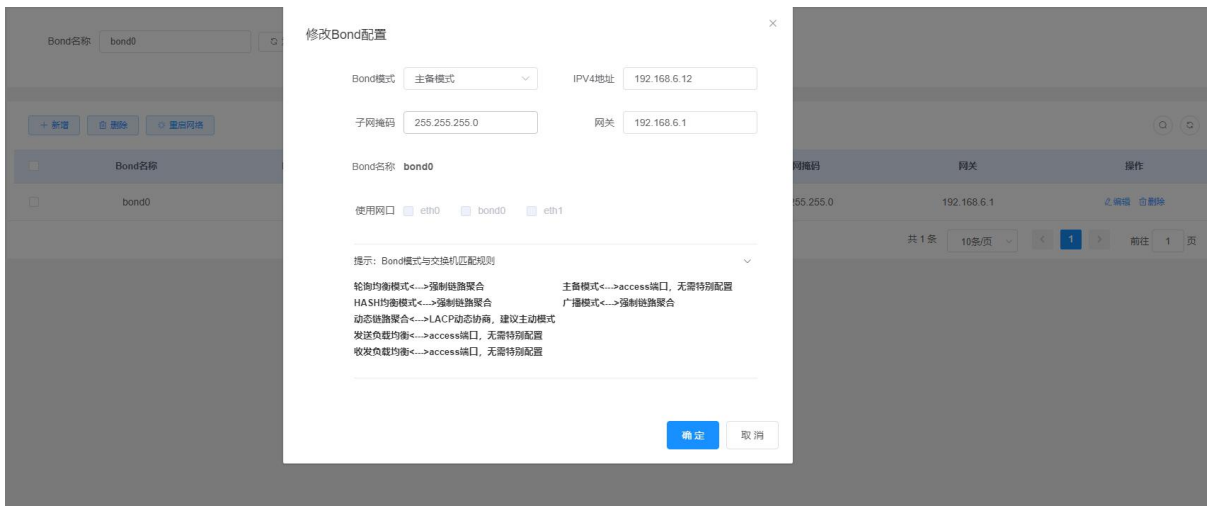
3.3.4.2.1. 新增

点击【新增】，在弹出的对话框中选择 Bond 模式、子网掩码，输入 IPV4 地址、网关、使用网口，点击【确定】。注意每个的格式都要填写正确。点击重启后生效。



3.3.4.2.2. 编辑

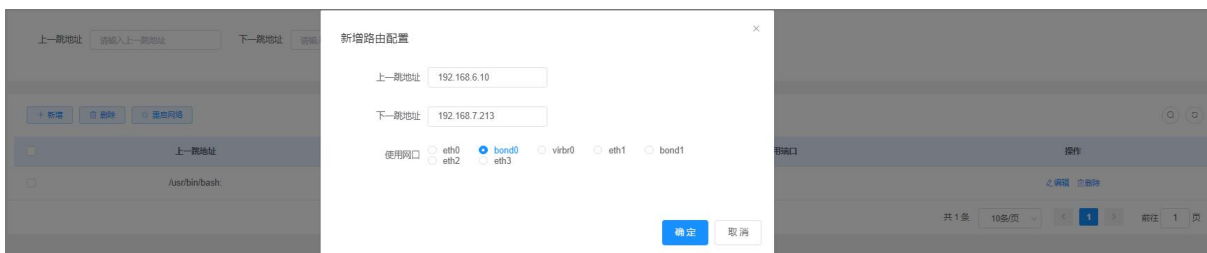
点击【编辑】，在弹出的对话框中可修改 Bond 模式、IPV4 地址、子网掩码、网关、使用网口，点击【确定】。注意每个的格式都要填写正确。点击重启后生效。



3.3.4.3. 路由配置

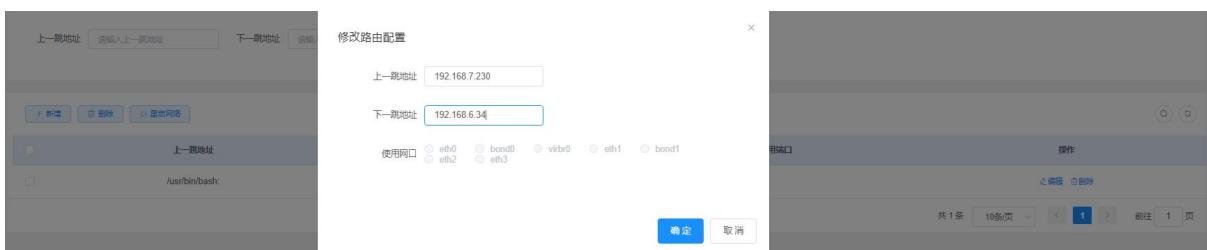
3.3.4.3.1. 新增

点击【新增】，在弹出的对话框中输入上一条地址、下一条地址、使用网口，点击【确定】。注意每个的格式都要填写正确。点击重启后生效。



3.3.4.3.2. 编辑

点击【编辑】，在弹出的对话框中可修改 bond 模式、IPV4 地址、子网掩码、网关、使用网口，点击【确定】。注意每个的格式都要填写正确。点击重启后生效。



3.3.4.4. 双机热备

3.3.4.4.1. 新增

点击【新增】，在弹出的对话框中输入虚拟组 id、虚拟地址、绑定模式、绑定网口、主机地址，点击【确定】。注意每个的格式都要填写正确。点击重启后生效。



3.3.4.4.2. 编辑

点击【编辑】，在弹出的对话框中可修改虚拟组 id、虚拟地址、绑定模式、绑定网口、主机地址，点击【确定】。注意每个的格式都要填写正确。点击重启后生效。



3.3.5. 时间配置

3.3.5.1. 授时卡配置

在此页面可启用授时卡同步、设置同步间隔，点击【立即同步】即可马上同步当前时间。注意 4G 信号强度和卫星信号强度是否可用。

授时卡配置

系统时间: 2023-03-02 20:01:34

上次同步时间: 2023-03-02 19:32:24

授时卡状态: 已安装未开启服务

启用授时卡同步: 关闭

同步间隔: 秒

卫星信号强度: ★ ★ ★ ★ ★ 不可用

4G信号强度: ★ ★ ★ ★ ★ 不可用

3.3.5.2. 系统时间配置

系统时间配置，可以设置当前系统时间，同步时间服务器上的时间，保证系统时间的精准性。勾选仅同步时间，则时间必须填写。勾选同步时区与时间，则必须填写时区、日期、时间。同步间隔和最大调整时间都得填写，保存配置后，系统时间每相隔指定时间将从 time.windows.com 时间服务器上同步一次。

系统时间配置 2023-03-02 20:02:12.934 [点击刷新](#)

与本地时间同步： 仅同步时间 同步时区与时间

时间：

启用NTP：

服务器名称	IP/域名	端口	首选服务器
server 0	192.168.6.134	13559	<input type="checkbox"/>

同步间隔 秒 (1-3600)秒, 缺省值: 300, 系统与NTP服务器同步的周期时间。

最大调整时间 秒 (1-3600)秒, 缺省值: 10, 0标识没有时间限制。

[保存配置](#)

3.3.6. 设备状态

3.3.6.1. 运行状态

运行状态包括服务状态和关机重启。点击服务状态的【启动】或者【停止】按钮，则会手动开启或者关闭服务。重启表示重新启动密码机服务器，关闭则关闭系统。

设备运行状态

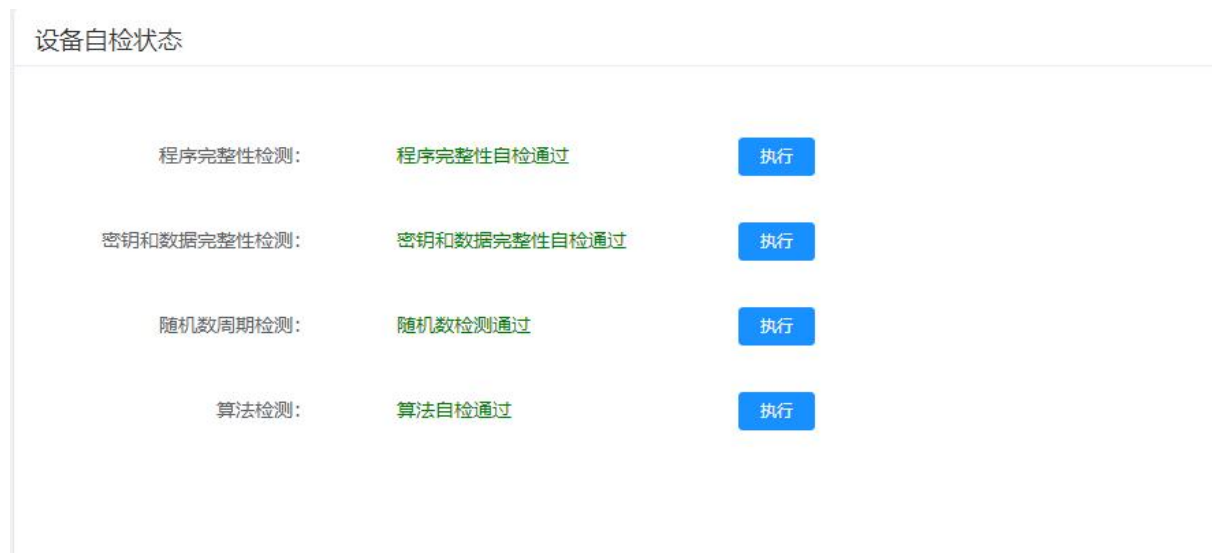
设备状态:	就绪状态		
服务运行状态:	已停止	启动	停止
NTP状态:	已开启	启动	停止
SNMP状态:	已开启	启动	停止
SSH状态:	已开启	启动	停止
重启服务器:	——	重启	——
关闭服务器:	——	——	关闭

3.3.6.2. 自检状态

程序完整性检测：检查程序完整性，防止程序中途被篡改，开机会检测，也可手动执行检测。

密钥和数据完整性检测：检测密钥和数据的完整性，防止数据和密钥中途被篡改，开机会检测，也可手动执行检测。

随机数周期检测、算法检测：随机数周期自检检查加密机系统随机数生成机制正常；算法自检检查加密机系统的算法是否正常。



3.3.7. 设备运维

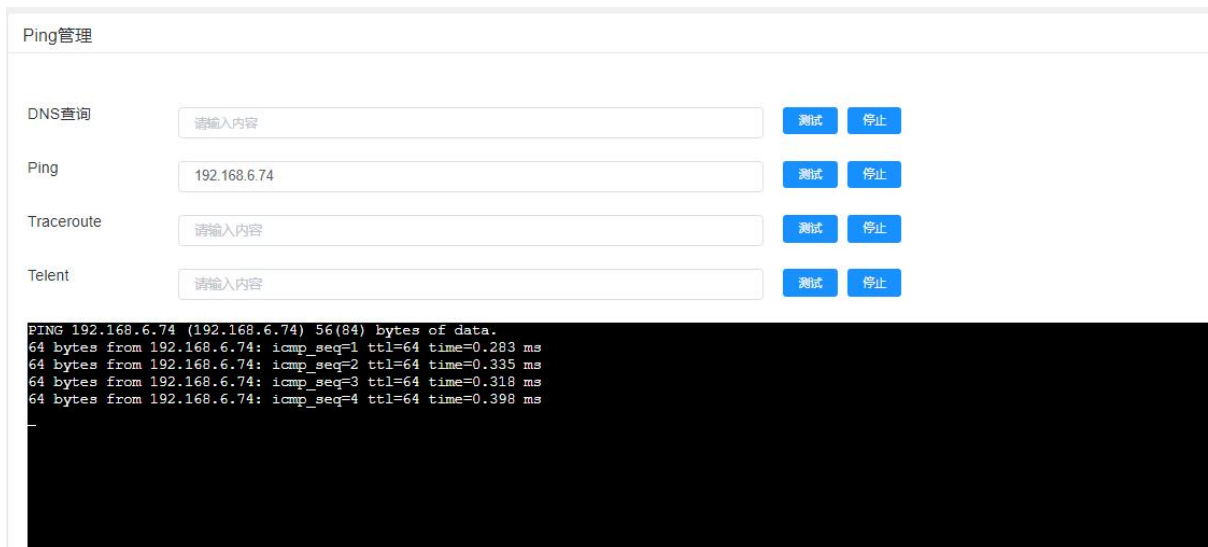
3.3.7.1. 运维功能

输入主机名、端口、用户名、密码，点击【连接】。注意端口号要输入正确。



3.3.7.2. Ping 功能

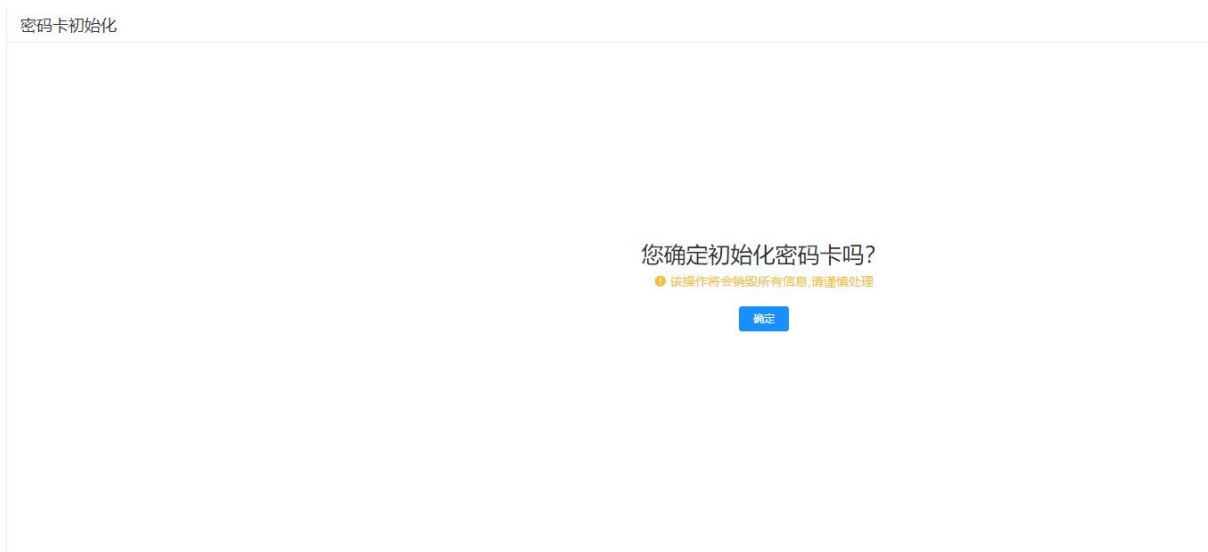
输入地址，点击【连接】。若中断连接，点击【停止】。



3.3.8. 设备重置

3.3.8.1. 密码卡初始化

如果确认初始化，则点击“初始化密码卡”按钮，初始化功能不可逆，请谨慎处理。注意初始化会将全部密钥和密码卡用户信息清空。



3.3.8.2. 恢复出厂设置

恢复出厂设置是将系统配置信息、网络配置信息、密码卡信息等所有配置将还原到初始化状态。注意恢复出厂设置会将整个系统重置，请谨慎操作。

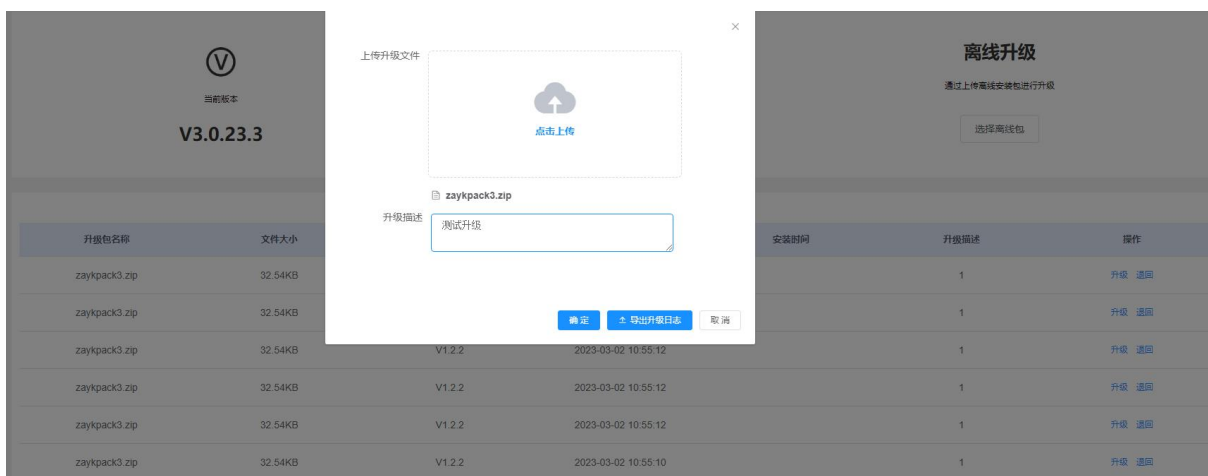
恢复出厂设置



3.3.9. 设备升级

3.3.9.1. 离线升级

点击【选择离线包】，然后上传安装包，输入升级描述，点击【升级】。注意升级的版本号会从离线包里面获取。



3.4. 审计管理员

3.4.1. 日志管理

3.4.1.1. 日志配置

日志配置页面如下图所示，可以配置日志记录等级，日志记录等级分为“错误、警告、信息、调试”，支持同步 **syslog** 日志功能，以及配置 **syslog** 所在服务器的 IP，接口。设置审计日志循环签名周期（小时），设置日志阈值。

日志配置

* 管理日志级别:

* 日志阈值: 条

* 是否备份到SYSLOG服务器: 是 否

* 服务器IP地址:

* 服务器端口号:

3.4.1.2. 日志查看

3.4.1.2.1. 查看、审计

管理日志、异常日志、服务日志、审计日志，可以根据选择的开始时间、结束时间。日志等级来过滤查询日志，从右侧多选框选择相对应的日志，点击“审计”按钮，即可对选择的日志进行审计。

日志编号 用户名

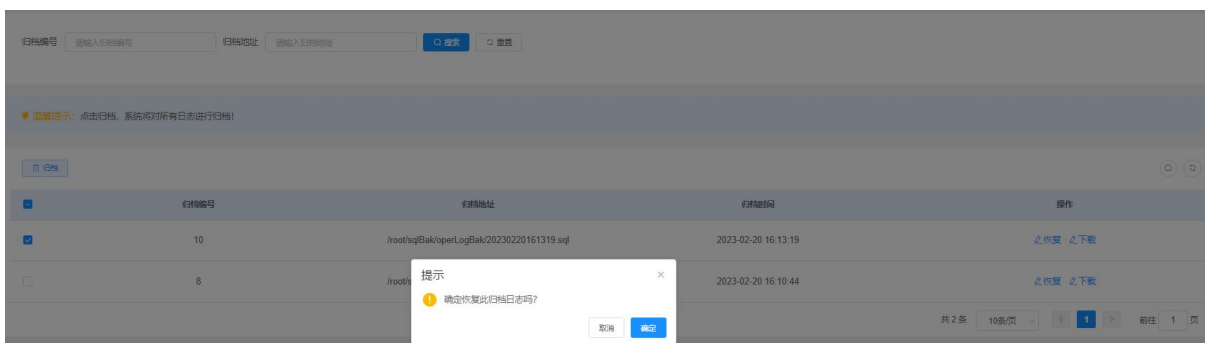
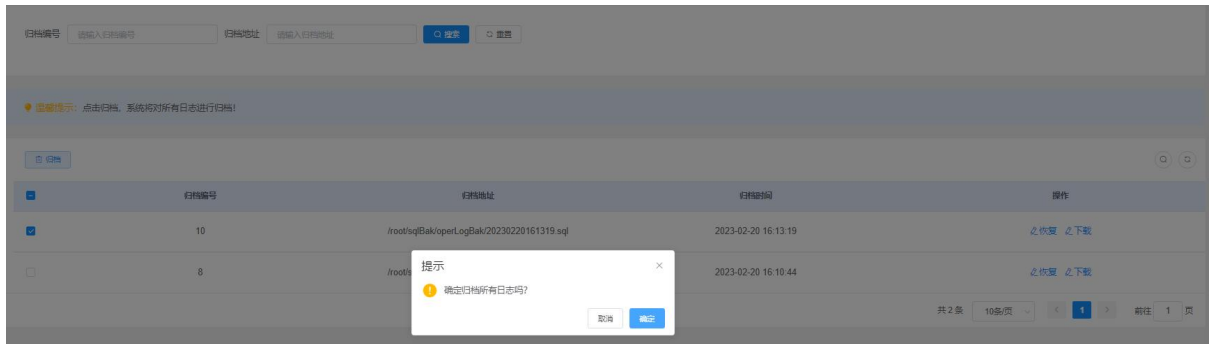
管理日志 异常日志 服务日志 审计日志

<input type="checkbox"/>	日志编号	用户名	创建日期	访问IP	详情	审计状态	操作
<input type="checkbox"/>	448	secAdmin		192.168.6.3	用户密码错误	未审计	去审计
<input type="checkbox"/>	393	sysAdmin		192.168.6.3	用户密码错误	未审计	去审计
<input type="checkbox"/>	345	admin		192.168.6.212	用户密码错误	未审计	去审计
<input type="checkbox"/>	332	admin	2023-02-22 11:43:03	127.0.0.1	用户密码错误	审计成功	去审计
<input type="checkbox"/>	330	admin	2023-02-22 11:43:01	127.0.0.1	用户密码错误	未审计	去审计
<input type="checkbox"/>	328	admin	2023-02-22 11:42:50	127.0.0.1	用户密码错误	未审计	去审计
<input type="checkbox"/>	327	admin	2023-02-22 11:42:38	127.0.0.1	用户密码错误	未审计	去审计
<input type="checkbox"/>	269	sysAdmin	2023-02-22 11:21:03	127.0.0.1	用户密码错误	未审计	去审计
<input type="checkbox"/>	268	sysAdmin	2023-02-22 11:20:57	127.0.0.1	用户密码错误	未审计	去审计

3.4.1.3. 日志归档

3.4.1.3.1. 归档和恢复

日志归档和日志恢复直接点击按钮即可，在弹出的对话框点击【确定】，即可完成操作。



3.5. 安全管理员

3.5.1. 设备导航

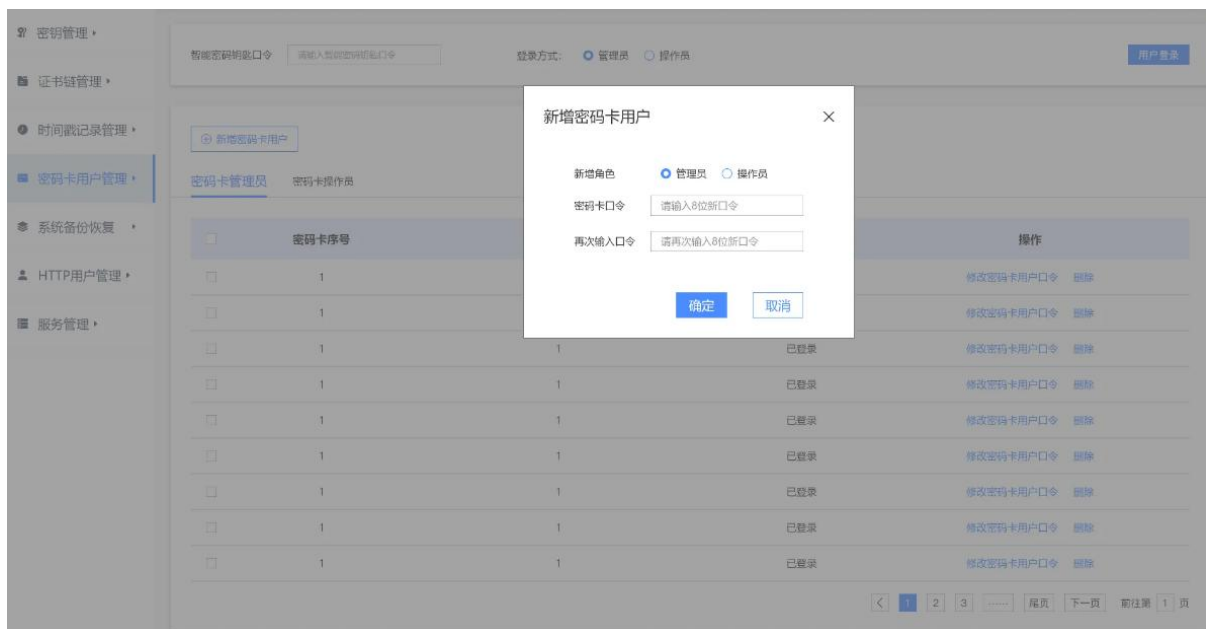
在此页面可以进行系统配置的快捷跳转。



3.5.2. 密码卡用户管理

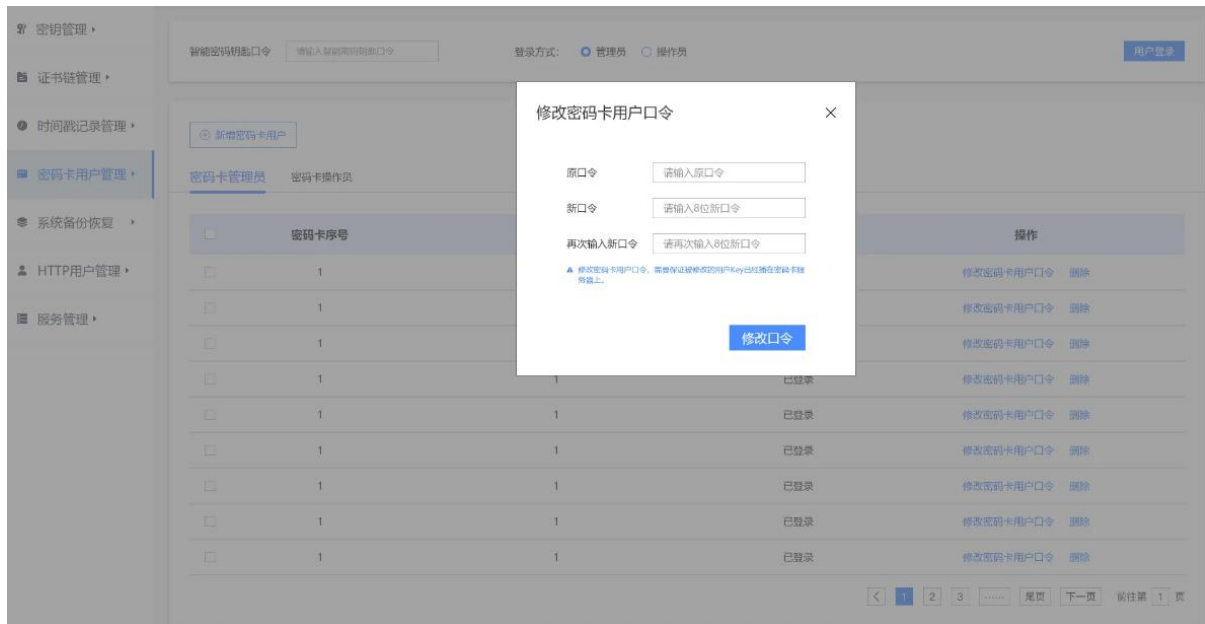
3.5.2.1. 新增密码卡用户

输入口令不得少于 6 位（数字、字母或者数字字母组合），作为操作员智能密码钥匙的口令。登录时采用智能密码钥匙+口令的双因子认证。此口令请妥善保管。输入口令后点击【点击新增密码卡用户】按钮，提示“操作员添加成功”。注意插入密码卡 UKey。



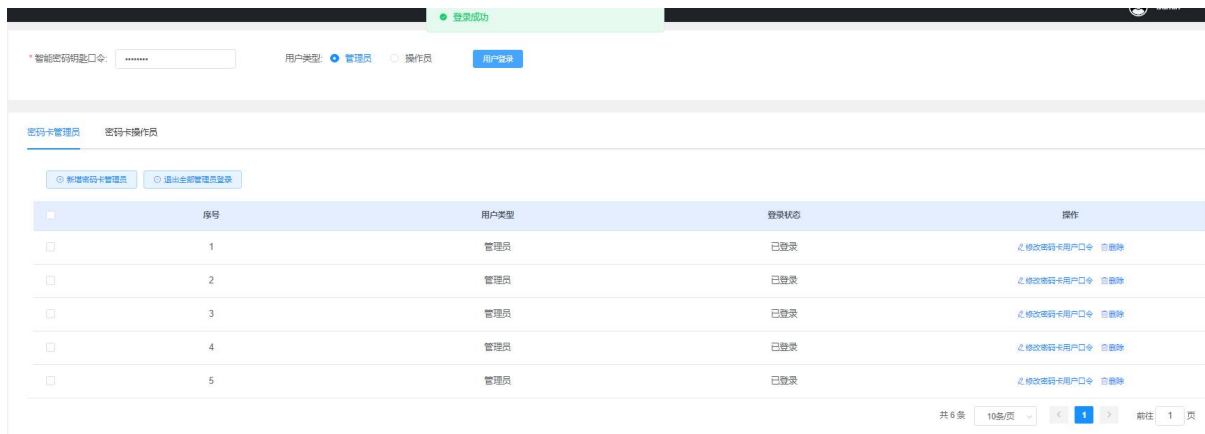
3.5.2.2. 修改密码卡用户口令

本功能可修改管理员或操作员智能密码钥匙的口令，修改后请妥善保管，以免遗忘。注意插入密码卡 UKey。



3.5.2.3. 登录

本功能会自动检测当前系统管理员、操作员数目，管理员登录（已登录），管理员未登录（未登录）即用户状态列表内显示登录状态，点击【退出全部管理员登录】，退出需要重新登录才能获得相应的权限。注意：插 Key 的时候要将管理员或者操作员的 Key 插入服务器带有钥匙标记的 USB 接口上。



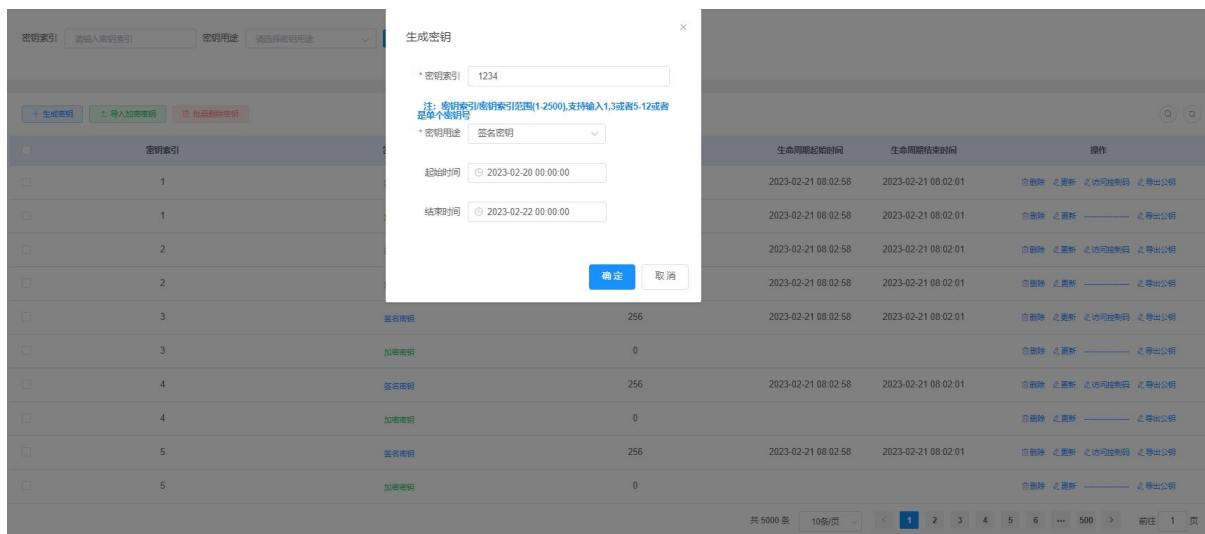
3.5.3. 密钥管理

3.5.3.1. SM2 密钥管理

3.5.3.1.1. 生成密钥

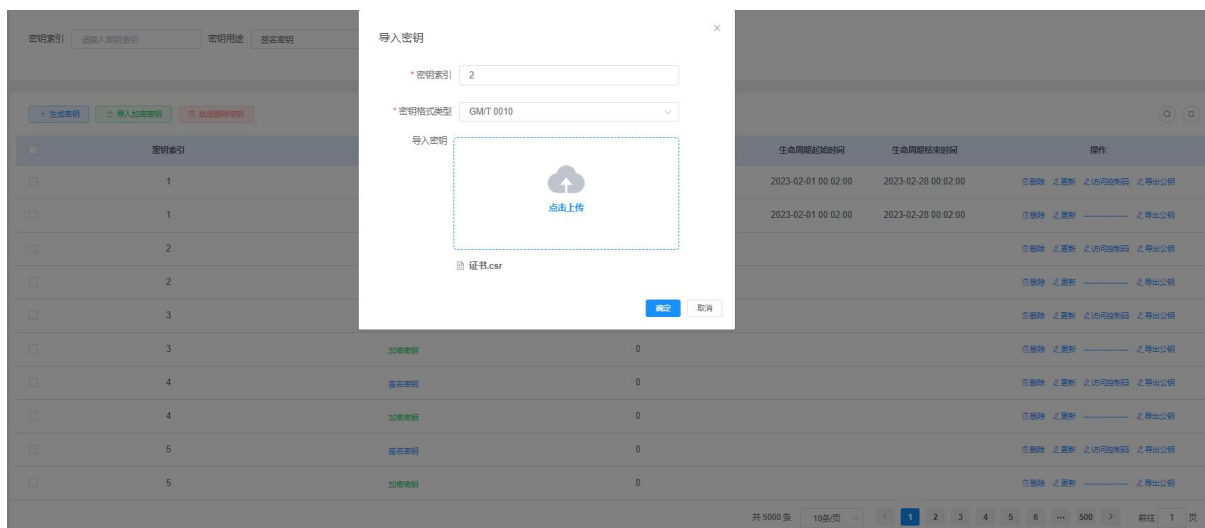
密钥标签内可输入密钥索引，密钥用途可选择签名密钥/加密密钥/签名和加密密钥，

密钥模长 256，设置生命周期（默认生效时间为当前），配置完成后点击【生成密钥对】按钮完成指定密钥的生成并安全保存。



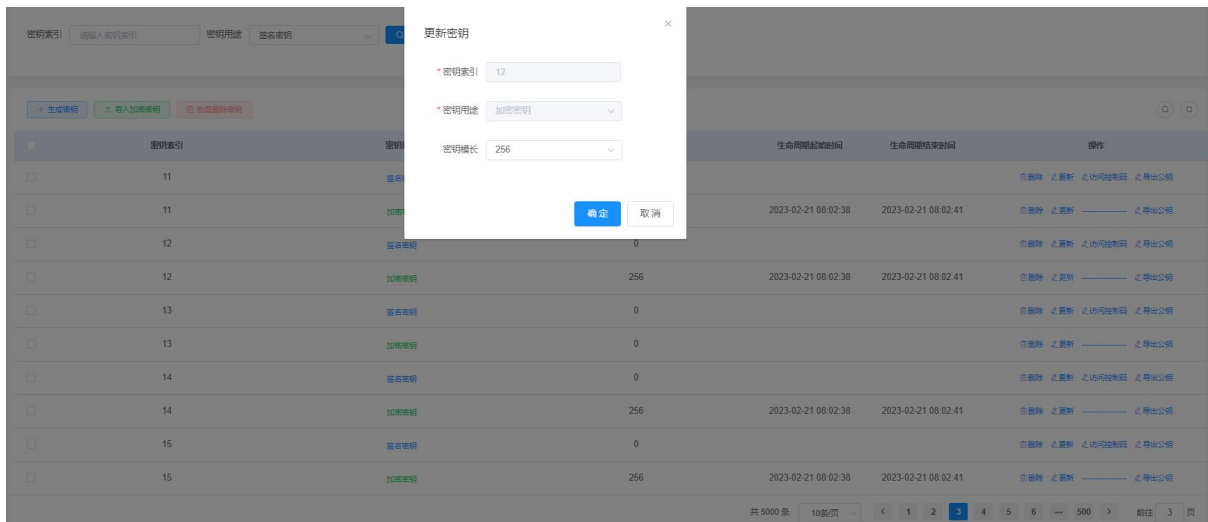
3.5.3.1.2. 导入加密密钥

点击【导入加密密钥】，输入密钥索引、选择密钥格式类型、选择文件，点击【确定】。



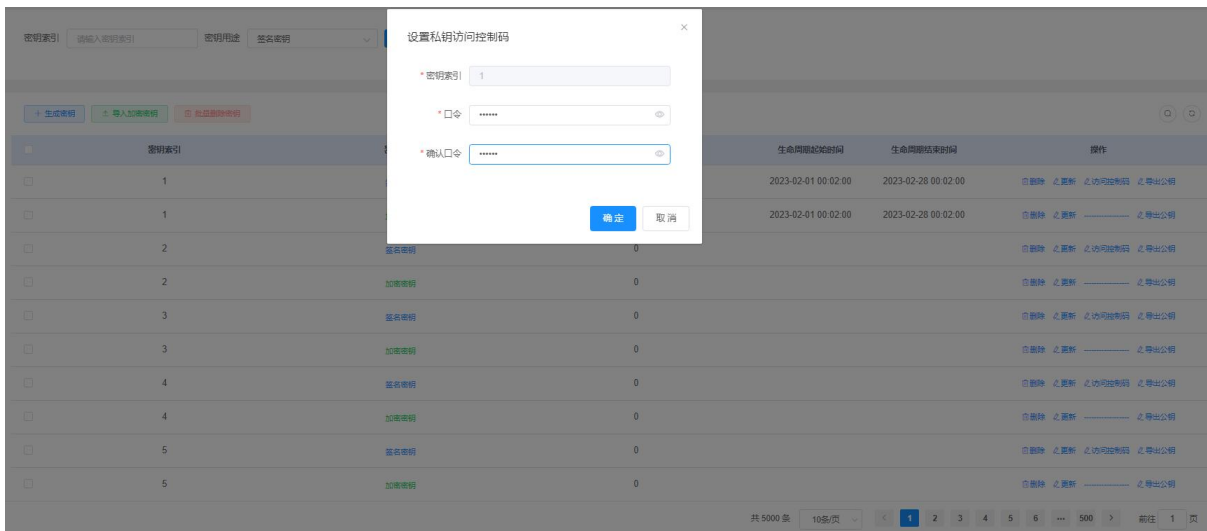
3.5.3.1.3. 更新

点击【更新】，在弹出的对话框中选择密钥模长，点击【确定】，修改用户对应的用户密钥模长。



3.5.3.1.4. 访问控制码

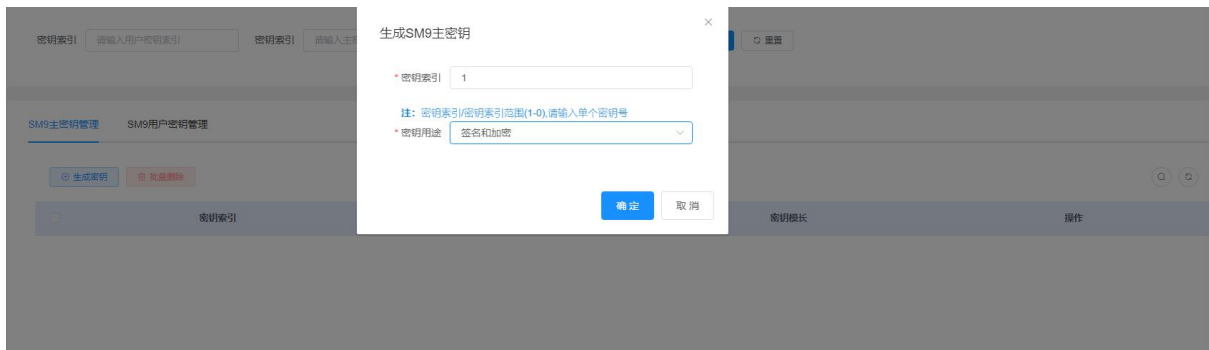
点击【访问控制码】，在弹出对话框中输入新口令、确认口令，点击【确认】。



3.5.3.2. SM9 密钥管理

3.5.3.2.1. 生成密钥

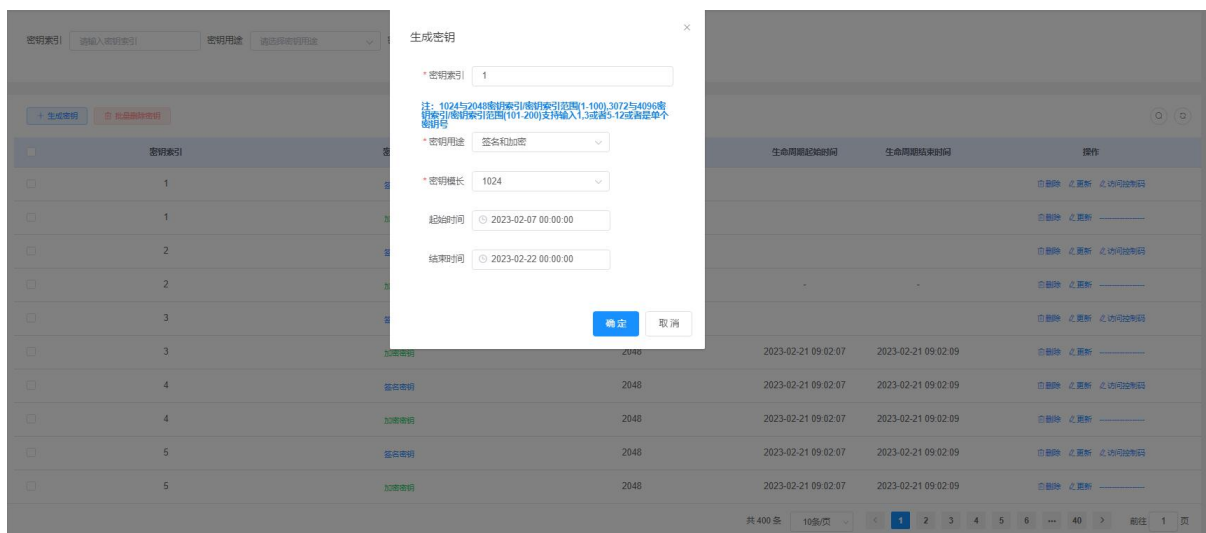
输入密钥索引和密钥用途，点击【确定】。



3.5.3.3. RSA 密钥管理

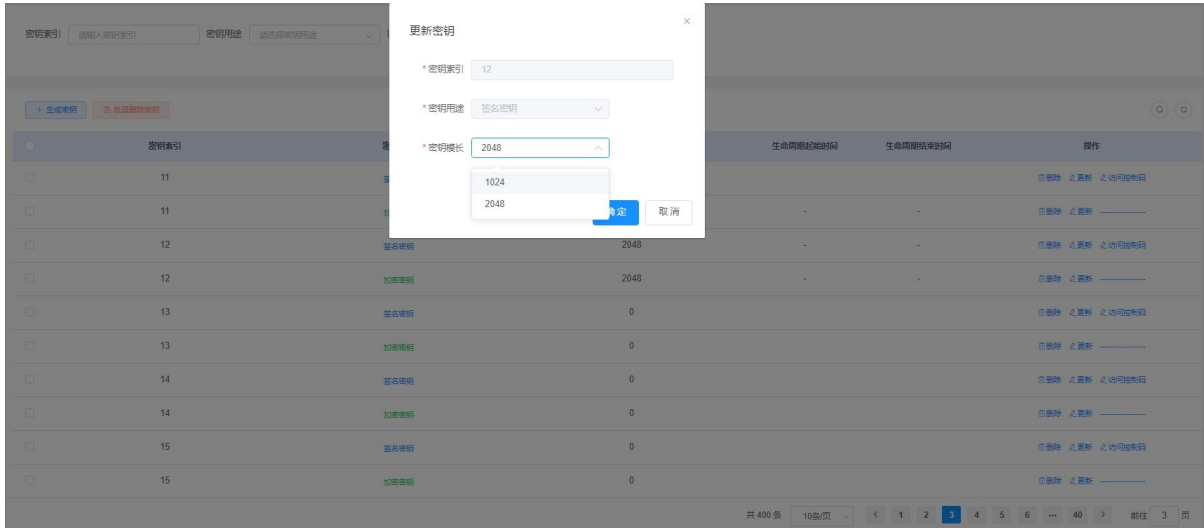
3.5.3.3.1. 生成密钥

密钥标签内可输入密钥索引，密钥用途可选择签名密钥/加密密钥/签名和加密密钥，密钥模长 1024，2048，设置生命周期（默认生效时间为当前），配置完成后点击【确定】按钮完成指定密钥的生成并安全保存。



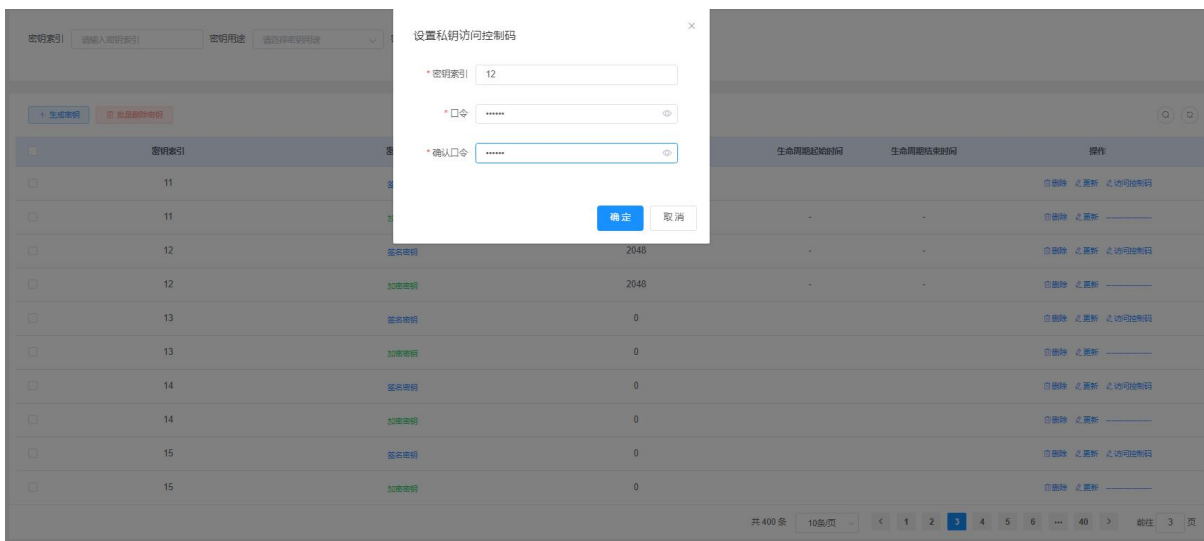
3.5.3.3.2. 更新

点击【更新】，在弹出的对话框中选择密钥模长，点击【确定】，修改用户对应的用户密钥模长。



3.5.3.3.3. 访问控制码

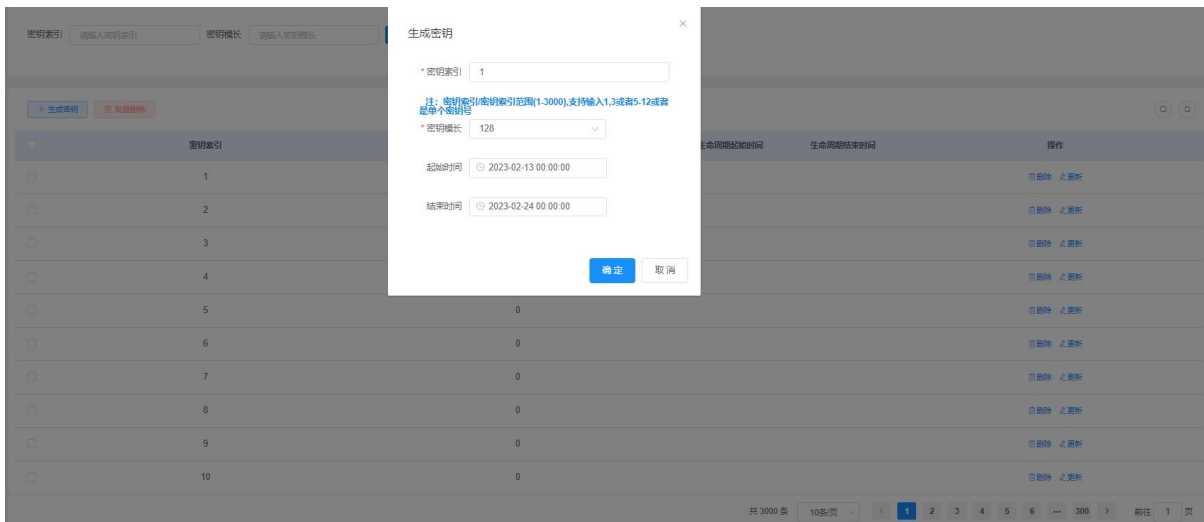
点击【访问控制码】，在弹出对话框中输入新口令、确认口令，点击【确定】。



3.5.3.4. 对称密钥管理

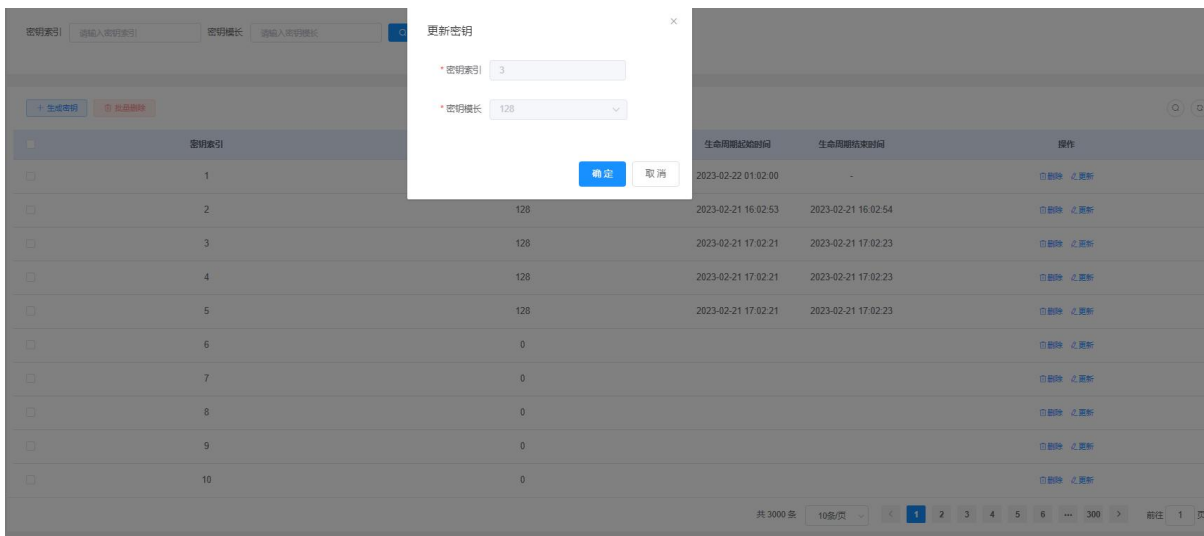
3.5.3.4.1. 生成密钥

密钥标签内可输入密钥索引，密钥长度可选择 128，设置生命周期（默认生效时间为当前）配置完成后点击【确定】按钮完成指定密钥的生成并安全保存。



3.5.3.4.2. 更新

点击【更新】，在弹出的对话框中选择密钥模长，点击【确定】密钥标签内可输入密钥索引，密钥长度可选择 128，设置生命周期（默认生效时间为当前）配置完成后点击【确定】按钮完成指定密钥的生成并安全保存。

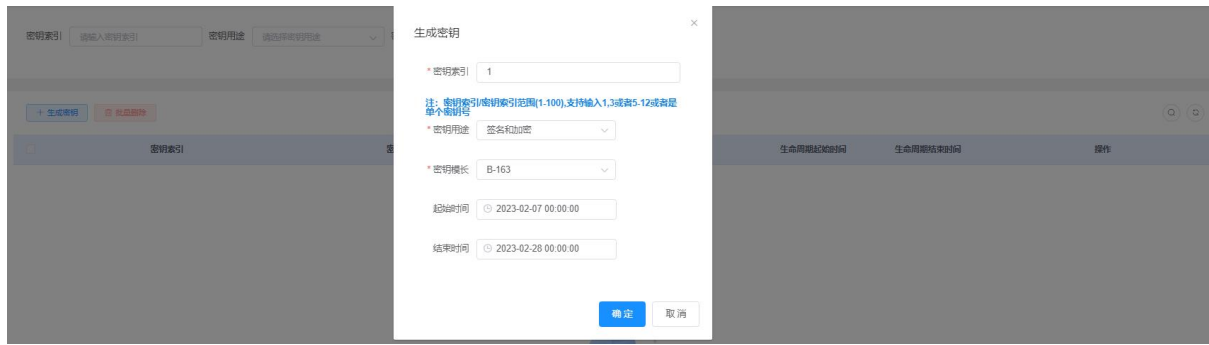


3.5.3.5. ECC 密钥管理

3.5.3.5.1. 生成密钥

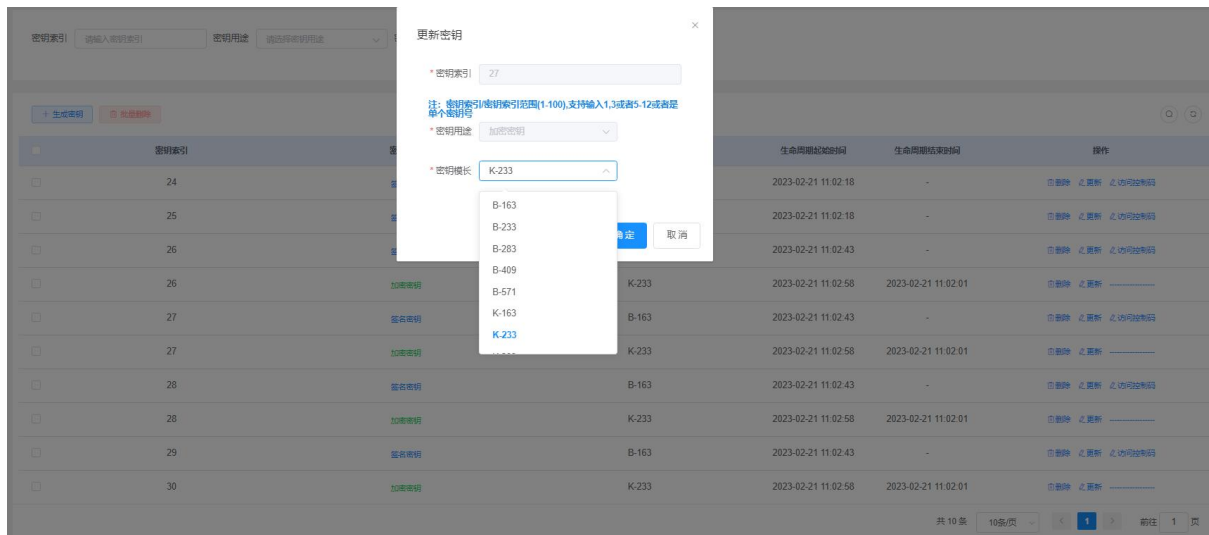
密钥标签内可输入密钥索引，密钥长度可选择 B-163, B-233, B-283, B-409, B-571, K-163, K-283, K-409, K-571, P-192, P-224, P-256, P-384, P-521, ED25519（默认 P-256）设置生命周期（默认生效时间为当前），配置完成后点击【确定】按钮

完成指定密钥的生成并安全保存。



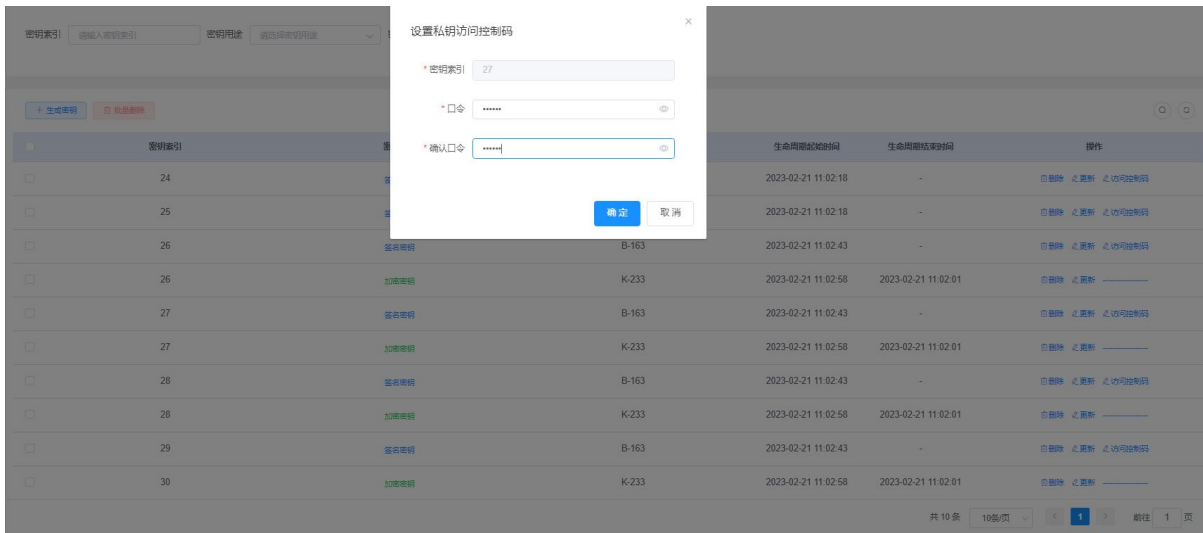
3.5.3.5.2. 更新

点击【更新】，在弹出的对话框中选择密钥模长，点击【确定】，修改用户对应的用户密钥模长。



3.5.3.5.3. 访问控制码

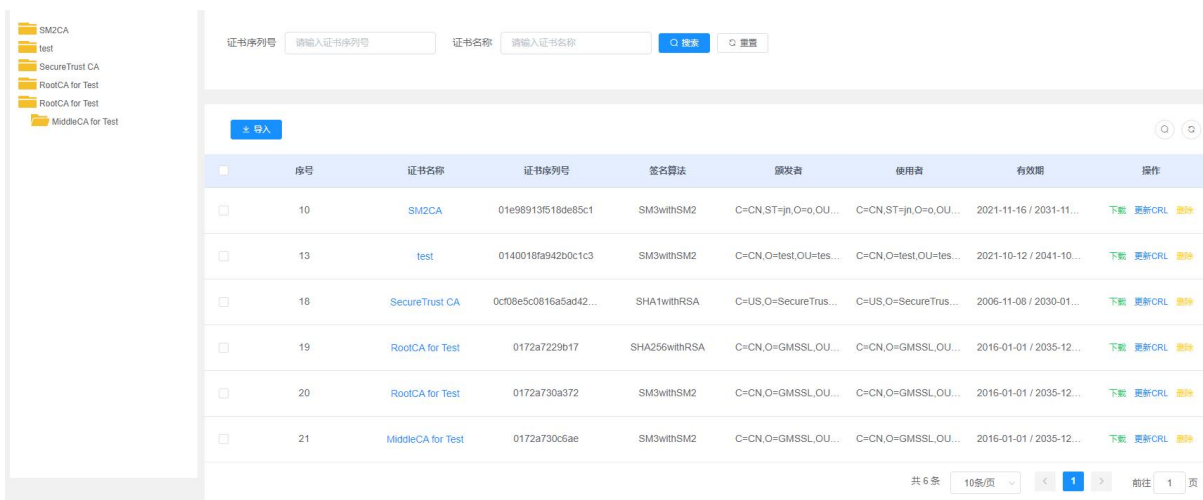
点击【访问控制码】，在弹出对话框中输入新口令、确认口令，点击【确认】。



3.5.4. 证书链管理

3.5.4.1. 根证书管理

可以导入根证书，下载根证书以及更新 CRL。注意导入证书的格式填写正确。



3.5.4.2. CRL 管理

可以导入 CRL，下载 CRL。注意导入 CRL 的格式填写正确。



3.5.4.3. 状态验证配置

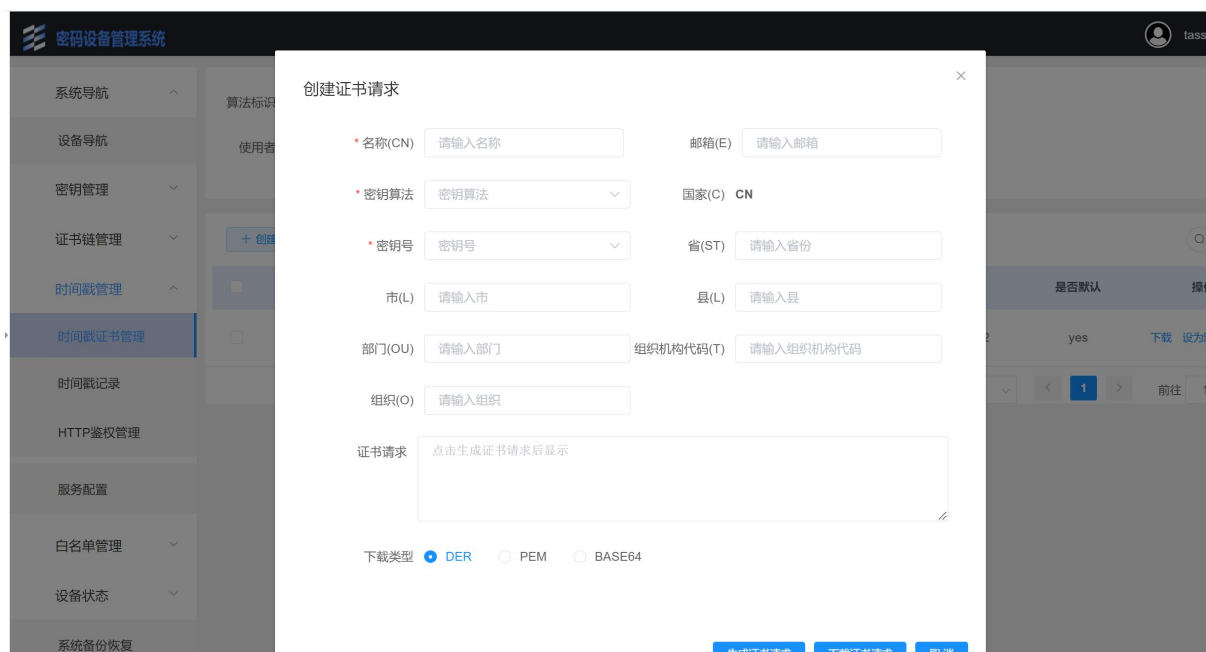
证书状态验证配置，点击相应的单选框，点击“提交”，设置证书状态验证配置。

3.5.5. 时间戳管理

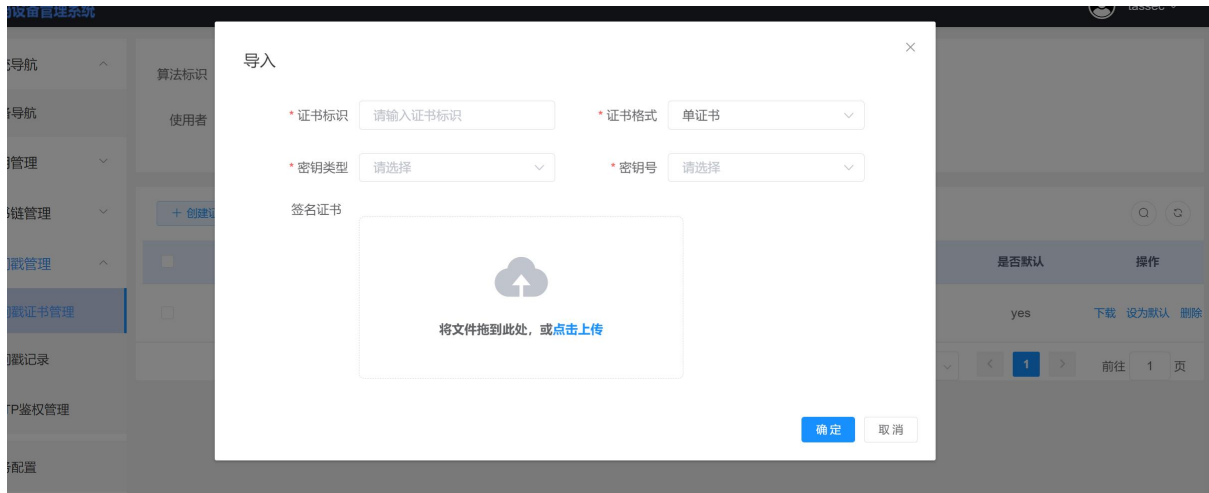
3.5.5.1. 时间戳证书管理

3.5.5.1.1. 创建证书请求

其主要功能为生成 PKCS10 证书请求。在界面中输入证书的主题信息并选择所用密钥后，点击【生成证书请求】按钮即可生成 PKCS10 格式的证书请求。证书请求的文件内容显示在 PKCS10 文本框中。管理员可以保存 PKCS10 后，去证书机构申请证书，然后导入到时间戳服务器中。



3.5.5.1.2. 导入时间戳证书



3.5.5.1.3. 设置默认证书



3.5.5.2. 时间戳记录

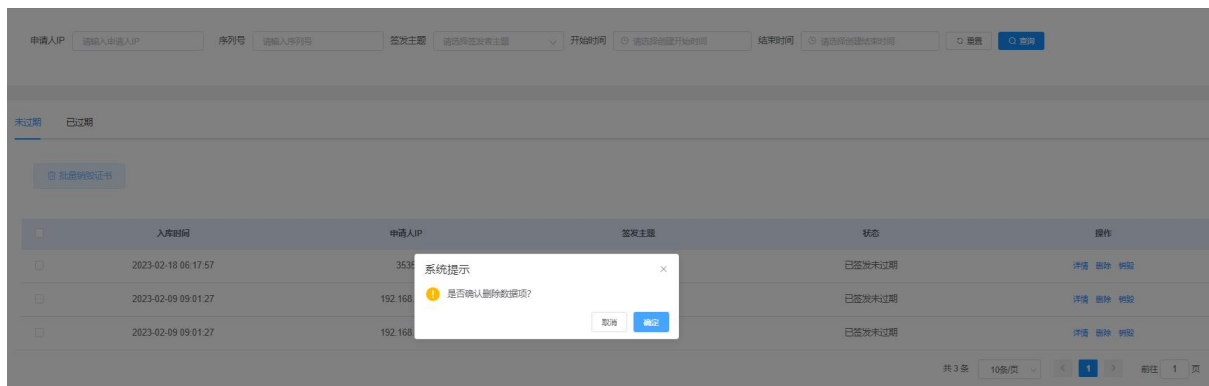
3.5.5.2.1. 详情

点击【详情】，即可查看时间戳的具体信息。



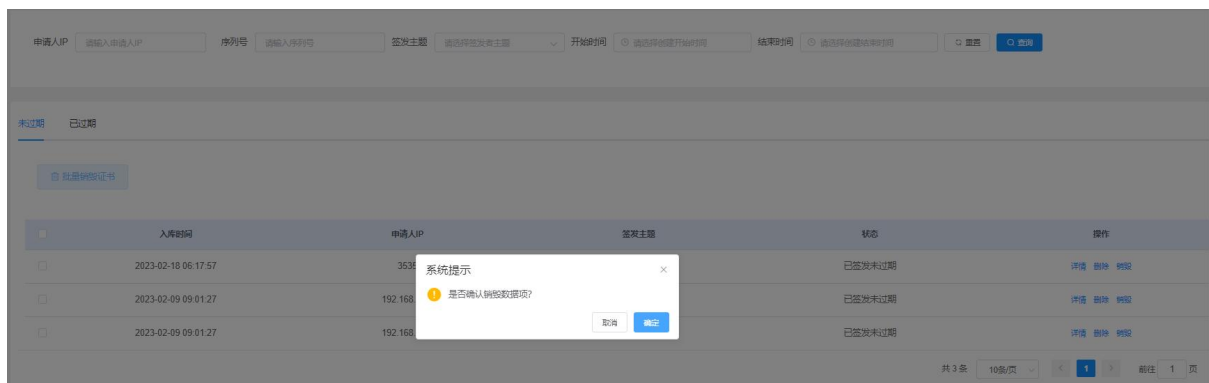
3.5.5.2.2. 删除

点击右侧的【删除】，删除相应的时间戳检索数据。



3.5.5.2.3. 销毁

点击【销毁】按钮，销毁相应的时间戳检索数据（时间戳生效后可执行成功）。

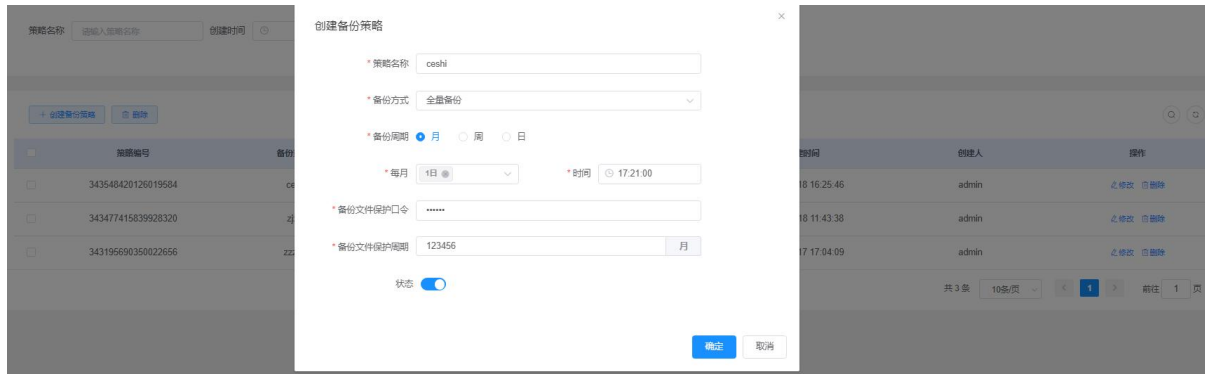


3.5.5.3. 时间戳备份

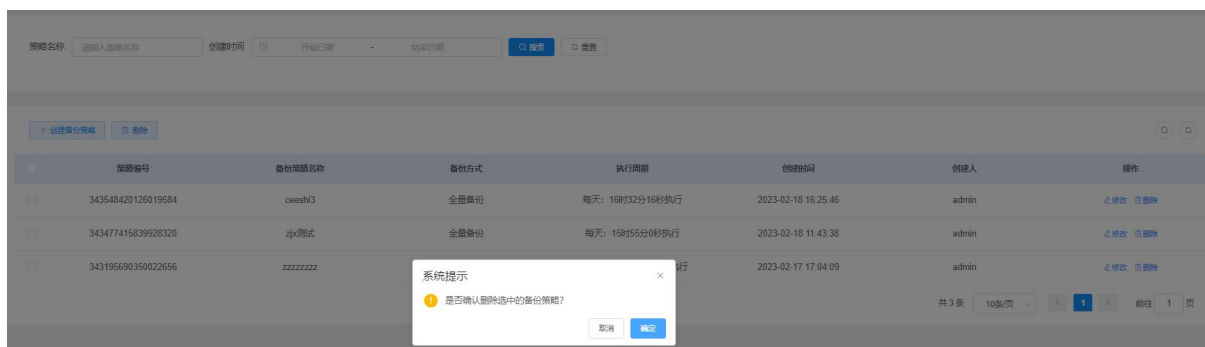
时间戳备份可以指定时间备份时间戳数据库，也可定期备份（相隔多少时间进行一次备份），备份数据库的名称、周期、口令都要填写，否则无法实现时间戳备份。

3.5.5.3.1. 备份策略

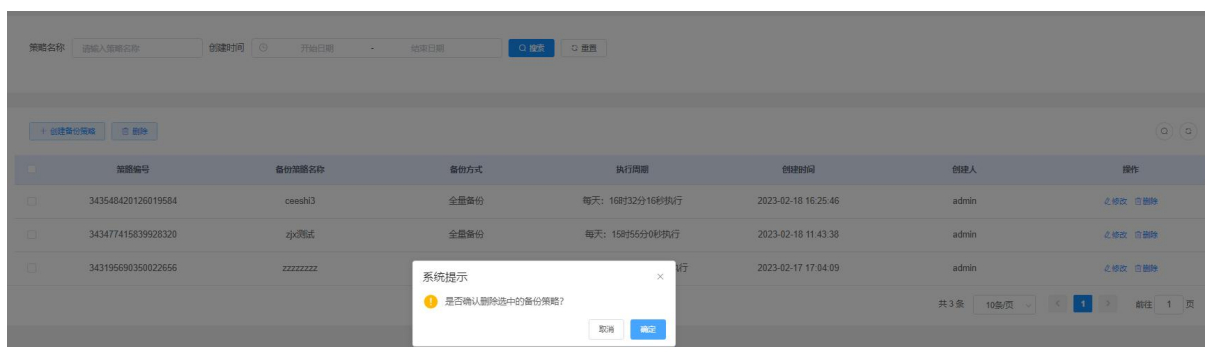
创建备份策略： 点击【创建备份策略】，在弹出的对话框中输入策略名称、备份方式、备份周期、每月/周/日、时间、备份文件保护命令、备份文件保护周期、状态，点击【确定】。



删除： 点击【删除】，在弹出的对话框中点击【确定】。



修改： 点击【编辑】，在弹出的对话框中，输入要修改的值，点击【确定】。



3.5.5.3.2. 备份文件

下载： 点击【下载】。

恢复文件： 点击【恢复】或者【恢复文件】，上传上一步的下载的文件，点击【确定】。



3.5.5.3.3. 备份恢复记录

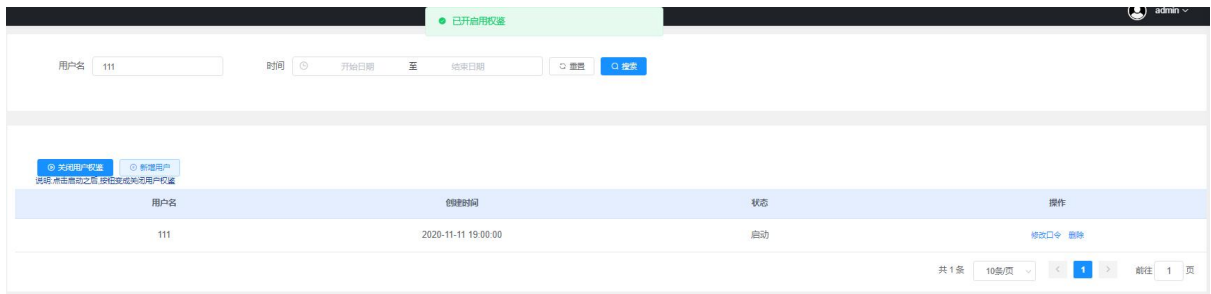
搜索： 在上方搜索栏中，输入相应的查询条件，点击【查询】，下方列表中即可展示出符合条件的记录。点击【重置】后搜索栏的条件将重置。

文件名称	操作类型	操作时间	同步状态	失败原因	结果	耗时
20230221全量备份-NO.343548420126019584	备份	2023-02-21 16:32:16	未同步		备份成功	0.03s
20230220全量备份-NO.343548420126019584	备份	2023-02-20 16:32:16	未同步		备份成功	0.04s
20230219全量备份-NO.343548420126019584	备份	2023-02-19 16:32:16	未同步		备份成功	0.04s
20230218全量备份-NO.343548420126019584	备份	2023-02-18 16:32:16	未同步		备份成功	0.03s
20230218全量备份-NO.343477415839928320	备份	2023-02-18 11:51:00	未同步		备份成功	0.04s
20230217全量备份-NO.343195690350022656	备份	2023-02-17 17:12:10	未同步		备份成功	0.09s
20230214全量备份-NO.342001680042299392	备份	2023-02-14 11:24:10	未同步		备份成功	0.22s
20230214全量备份-NO.342001680042299392	备份	2023-02-14 11:21:10	未同步		备份成功	0.21s
20230214全量备份-NO.342001680042299392	备份	2023-02-14 11:17:10	未同步		备份成功	0.22s
20230214全量备份-NO.342001680042299392	备份	2023-02-14 11:13:10	未同步		备份成功	0.19s

3.5.6.HTTP 鉴权管理

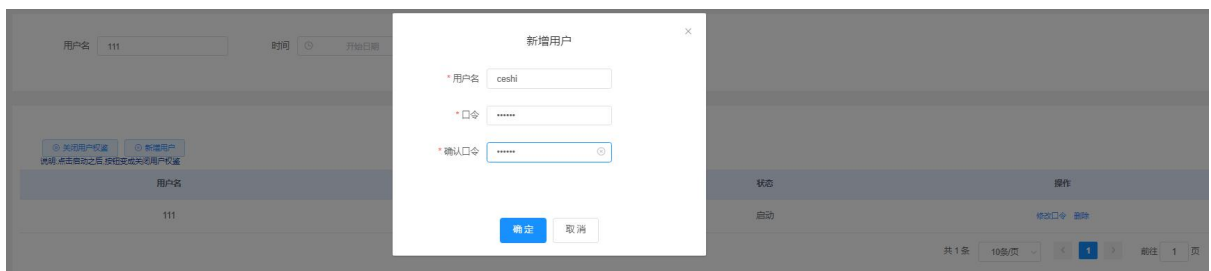
3.5.6.1. 启用、关闭用户鉴权

点击【启用/关闭用户鉴权】，即可完成相应的功能操作。



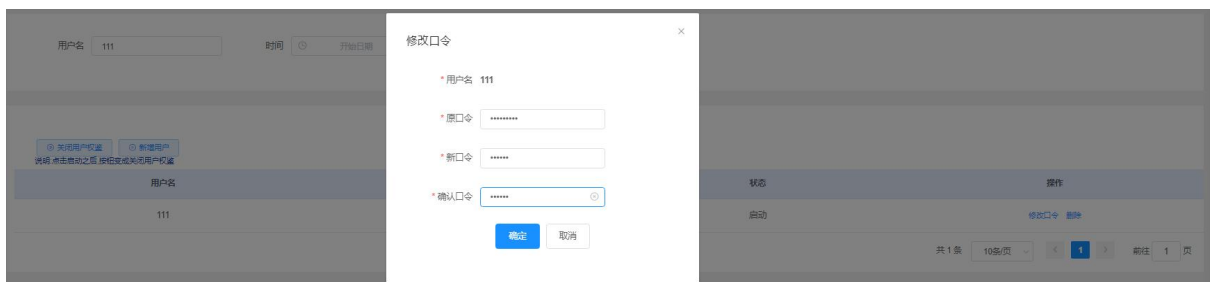
3.5.6.2. 新增用户

点击【新增用户】，输入用户名、口令、再次输入口令，点击【确定】。



3.5.6.3. 修改口令

点击【修改口令】，在弹出的对话框中输入原口令、新口令、确认口令，然后点击【确定】。



3.5.7. 服务配置

服务配置主要修改服务配置信息，包括服务器密码机端口最大数量、服务器密码机端口配置数量、服务器密码机端口，输入完信息后，点击【确认】，点击【重启服务】，使修改的配置生效。

服务器密码机 签名验签服务器 时间戳服务器

服务器密码机端口最大数量 3

服务器密码机端口配置数量 请输入服务器密码机端口配置数量 确认

* 服务器密码机端口0 13552

确认 重启服务

3.5.8. 白名单管理

添加白名单会指定 IP 访问，不配置白名单，所有 IP 都可以访问。

点击“新增”按钮，会出现新增白名单地址弹窗，类型可以选择单地址、子网、地址段。

类型选择单地址就是添加单个 IP 地址。

新增服务白名单

类型 请选择类型

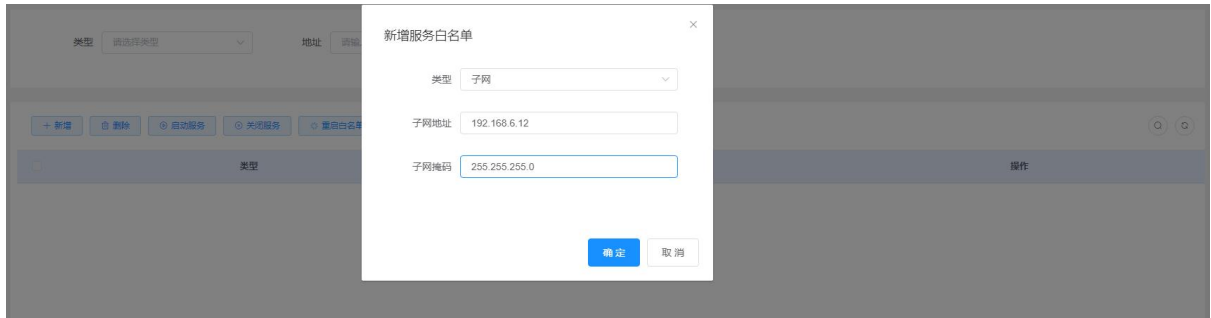
地址

类型 单地址

地址 192.168.6.11

确定 取消

类型选择子网，需要填写子网地址、子网掩码。



地址段需要填写起始地址、结束地址，支持 IP 地址段最后一位的起止 IP 地址群添加，如 192.168.6.10-192.168.6.20，表示添加 IP 地址在 192.168.6.10-192.168.6.20 之间的所有地址（包括 192.168.6.10、192.168.6.20）。



注意新增、编辑、删除都需要重启白名单。

3.5.9. 设备状态

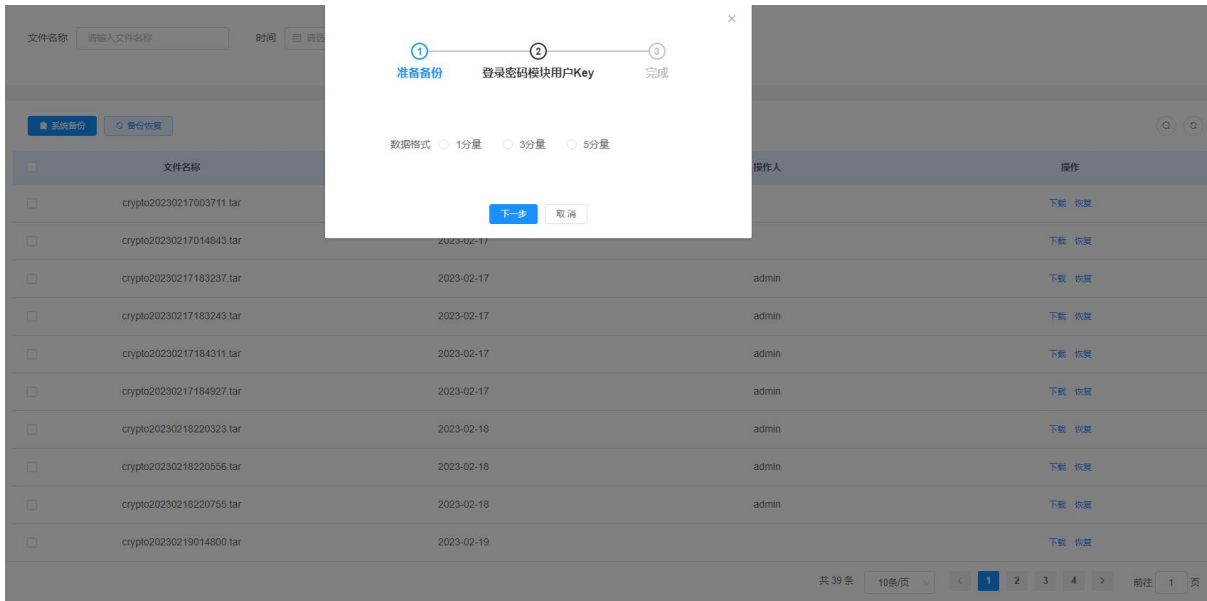
详见本文档 3.2.6 章节。

3.5.10. 系统备份恢复

3.5.10.1. 系统备份

系统备份，主要对系统的数据库、密钥、以及文件系统进行加密之后备份，备份之后下载到本地供系统恢复使用。

注意，备份之前要确认密码卡权限满足，至少登录半数以上管理员，验证备份 key。



3.5.10.2. 系统恢复

系统恢复，将系统备份的文件上传至密码机服务器。

点击浏览选择要上传的恢复文件，点击上传进入下一步。

注意，按照提示依次插入管理员恢复 key，最后一步需要较长时间，请耐心等待。完成后会提示“恢复成功”。

