翼安签名验签服务器
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 概述 1
1.1 简介 1
2 产品安装说明 1
2.1 安装环境要求 1
2.2 产品安装 1
3 产品操作说明 1
3.1 应用实体管理 9
3.2 数据备份恢复 20
3.2.1 数据备份 20
3.2.2 数据恢复 24
3.3 双机热备管理 28
3.4 用户管理 31
3.4.1 系统用户管理 31
3.4.2 restful用户管理 37
3.5 设备管理 41
3.5.1 初始化 41
3.5.2 系统升级 43
3.5.3 设备信息 43
3.5.4 重启/关机 44
3.5.5 系统配置 45
3.5.6 时间源设置 53
3.5.7 服务管理 55
3.5.8 设备自检 56
3.6 证书管理 57
3.6.1 证书查询设置 57
3.6.2 CA证书管理 58
3.6.3 CRL管理 59
3.6.4 用户证书管理 61
3.6.5 设备证书管理 62
3.6.6 证书验证管理 68
3.6.7 证书同步设置 69
3.6.8 数字信封管理 70
3.7 日志管理 72
3.7.1 日志设置 72
3.7.2 日志审计（仅审计员可见） 74
3.7.3 故障日志 79
3.8 预警管理 82
3.8.1 预警设置 82
3.8.2 预警列表 83
3.9 国标密钥管理 85

3.9.1 SM2密钥.....85
3.9.2 RSA密钥.....87
3.9.3 对称密钥.....90
3.9.4 密钥批量管理.....92
3.9.5 私钥权限码.....94
4 初始化配置签名验签使用步骤..... 95
5 常见问题及解答..... 96

1 概述

1.1 简介

签名验签服务器严格按照国家密码管理局 GM/T 0029-2014《签名验签服务器技术规范》等技术规范进行设计，产品已取得国家密码管理局商用密码检测中心颁发的商用密码产品认证证书，支持国家密码管理局认可的密码算法，能够为各类系统提供数据签名和验签、基于数字证书的身份认证、基于数字证书的加解密等安全保护，以保证关键业务信息的真实性、完整性和不可否认性。产品可以应用于电子商务、CA 认证中心、网上银行等服务器端，提供高强度和高效率的密码服务。

2 产品安装说明

2.1 安装环境要求

产品为 2U 机架式服务器,安装前须准备 2U 机位、2 个 AC220V/50Hz 交流电源插座、设备接入网络环境（设备 IP 地址、路由、安全策略等）。

2.2 产品安装

签名验签服务器部署在局域网内，只为局域网内的应用实体和用户服务，不能接入互联网，为局域网外的用户使用。

设备部署可以是一台应用服务器对应一台签名验签服务器,也可以一对多、多对一、多对多。

3 产品操作说明

将测试 PC 的 IP 配置为 192.168.3.*网段后，浏览器访问 https://192.168.3.3，进入登录页面。系统首次打开登录页面如 0,**默认登录用户名 fisherman,口令 fisherman 及验证码。**

注意：此处默认登录用户名及口令为可配置，即可根据实际情况自定义默认用户名及口令。

图3-1 默认登录页面

首先点击【**下载工具**】，如0，弹出后下载Setup.exe程序。执行安装程序完成组件安装。如0。

图3-2下载工具

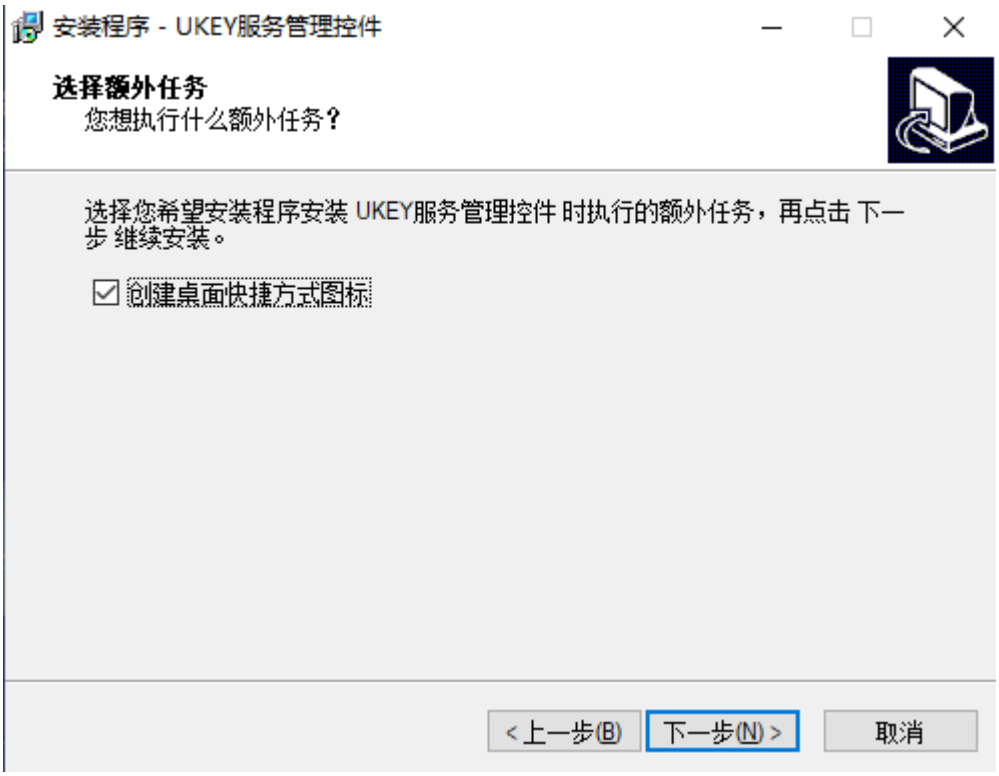

图3-3安装程序

安装完成后重新刷新网页，输入验证码后，点击【登录】按钮即可登录。如 0。

图3-4默认用户登录

用户默认用户登录之后进入首页，如图3-5。该页面显示当前系统的基本信息，主要包括以下四项：

数量信息：

显示用户数量、证书数量、实体数量和并发连接数。

系统状态：

显示管理员访问次数统计和系统资源占用情况。

网络状态：

显示当前设备各网口的网络状态。

模块状态：

显示设备的加密卡状态。

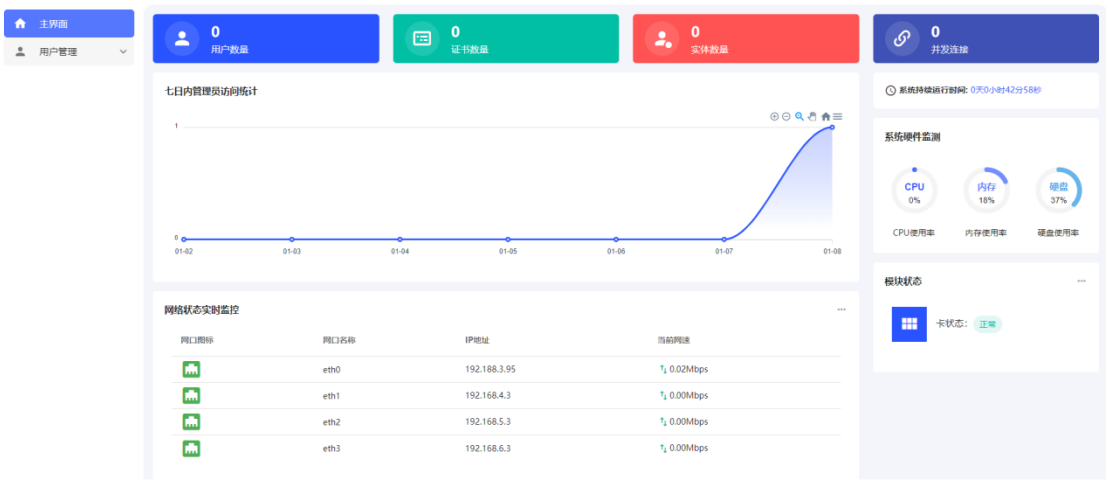

图3-5 默认用户首页

点击左侧导航栏【用户管理】下的【系统用户管理】菜单添加新用户，如0。点击“新建用户”按钮，插入UKEY到电脑，点击“刷新”会在用户令牌显示插入的UKEY序列号，如图3-7。

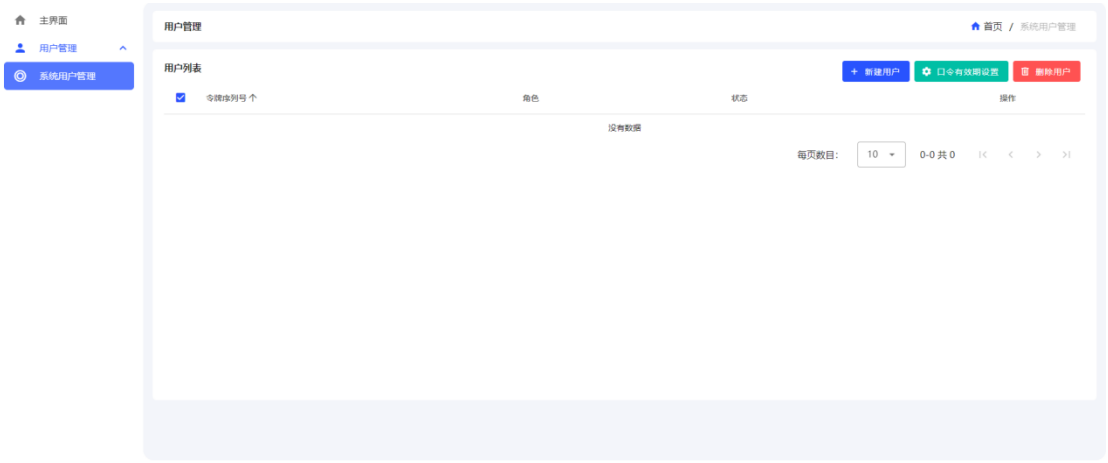

图3-6系统用户管理

图3-7新建用户

输入令牌口令（默认口令12345678），选择该用户是【管理员】、【操作员】还是【审计员】，点击【确定】按钮完成用户添加。如0。

图3-8新建用户

在系统用户管理功能中创建管理员、操作员、审计员用户，并绑定Ukey后，点击右上角用户图标，选择“退出系统”如0，退出默认用户访问界面，再次进入系统登录页面，如0。

图3-9退出系统

图3-10 登录页面

选择要登录的UKEY序列号，输入UKEY口令和验证码，点击【登录】。管理员登录成功之后进入管理员界面首页，如0。

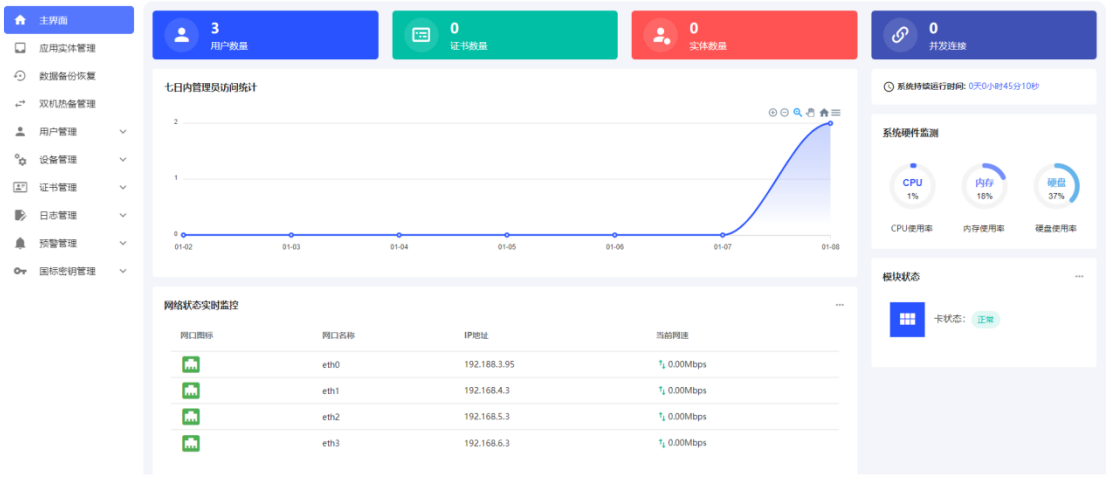

图3-11 管理员首页

操作员登录成功之后进入操作员管理首页，如0。

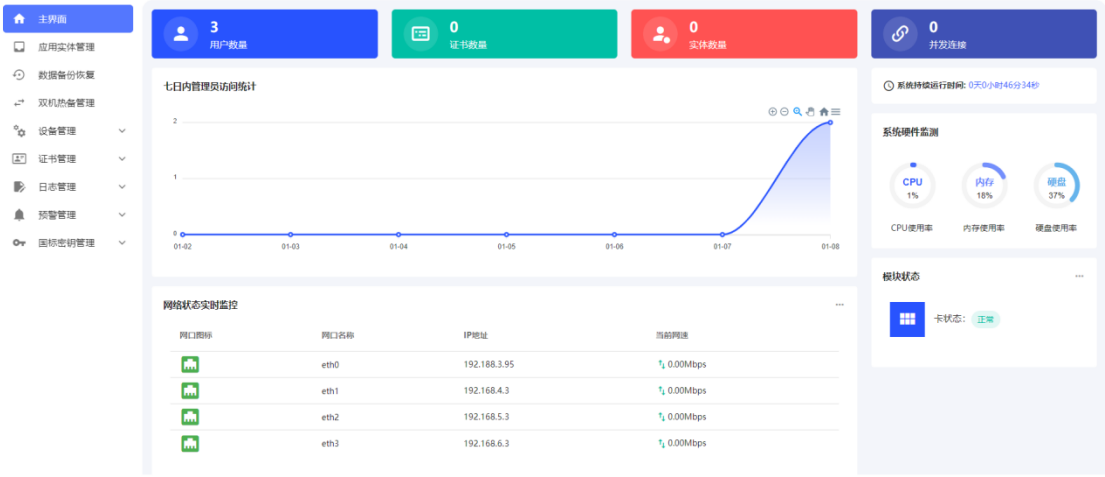

图3-12 操作员首页

审计员登录成功之后进入审计员管理首页，如0。

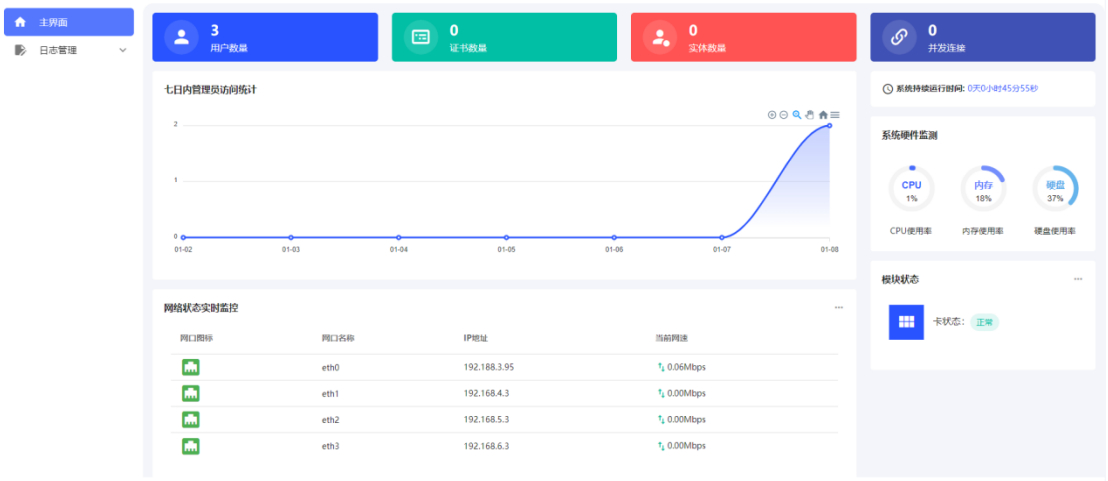

图3-13 审计员首页

点击右上角用户图标，除了可对当前登录用户进行退出外，还可进行密码修改操作，点击“修改密码”，弹出修改界面如0。输入原口令以及新口令之后，点击确定即可完成密码修改。

图3-14 修改口令

3.1 应用实体管理

应用实体管理页面显示应用实体的基本信息，包括应用实体名、密钥类型、密钥索引号、密钥长度、签名证书状态、加密证书状态、加密密钥对状态、应用实体状态，界面如 0。

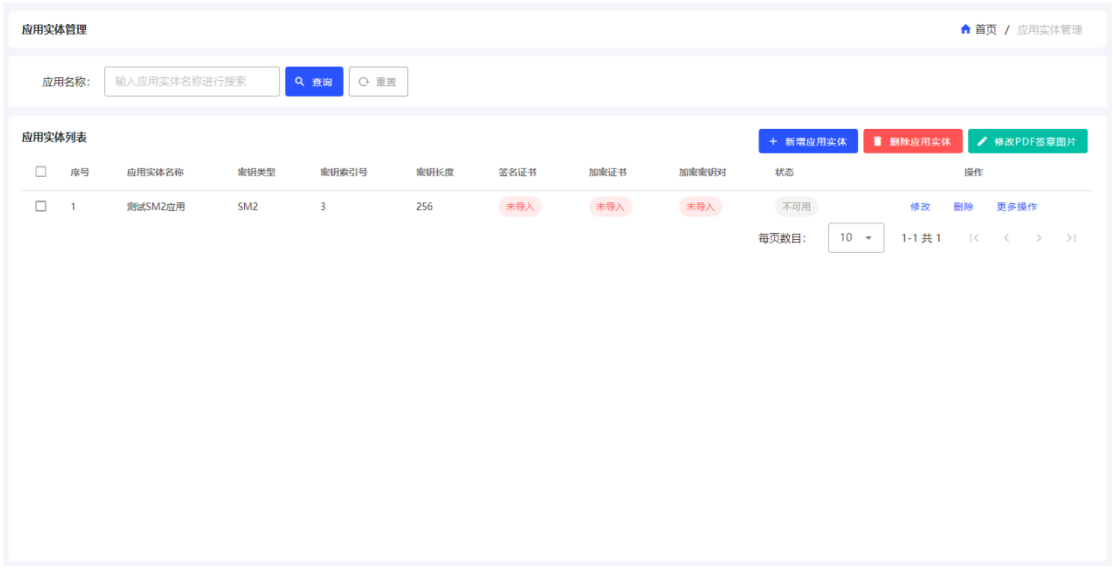

图3-15应用实体注册

新增应用实体时，点击“新增应用实体”按钮，选择密钥类型，输入应用名称、私钥权限码、密钥索引号，点击【确定】。界面如 0。

图3-16新增应用实体

点击【确定】即可完成应用实体的注册，应用实体对应密钥号的私钥权限码也会被创建，此时会弹出“创建应用实体完成，但不可用，请在应用实体信息管理中完成其他操作”，需要导入证书应用实体才可用。界面如 0。

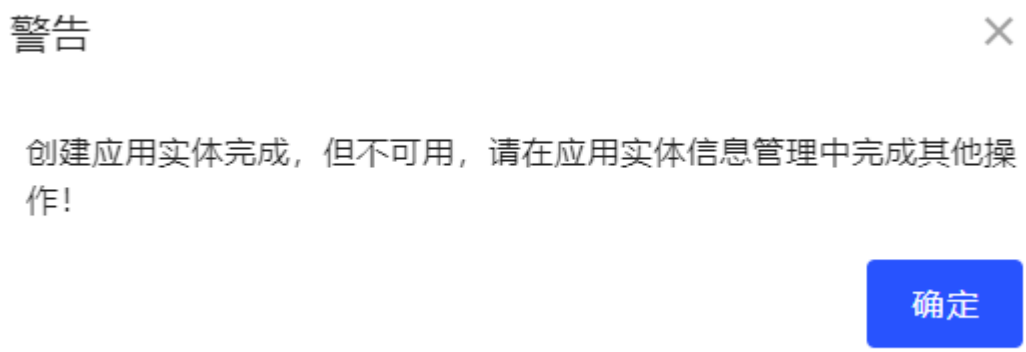

图3-17应用实体注册弹出框

应用实体列表显示所有注册的应用实体信息，包括应用实体信息的修改、签名/加密证书的 P10 生成请求、签名/加密证书、加密密钥对的导入、签名/加密证书的下载、pdf 签章验签、删除功能，界面如 0。

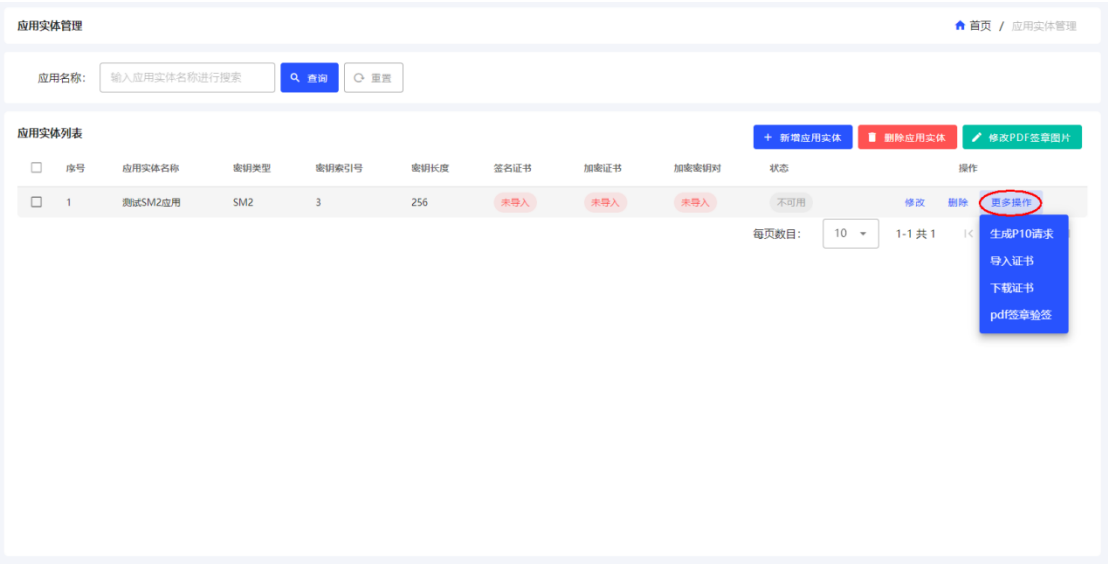

图3-18应用实体功能操作

在想要操作的应用实体上，点击“修改”，弹出对话界面，如 0，输入想要修改的密钥类型、应用名称、私钥权限码、密钥索引号，点击确定，即可完成应用实体信息的修改操作。

图3-19应用实体修改

在想要操作的应用实体上，点击“删除”，弹出对话界面，如 0，点击“确定”，即可删除对应的应用实体。

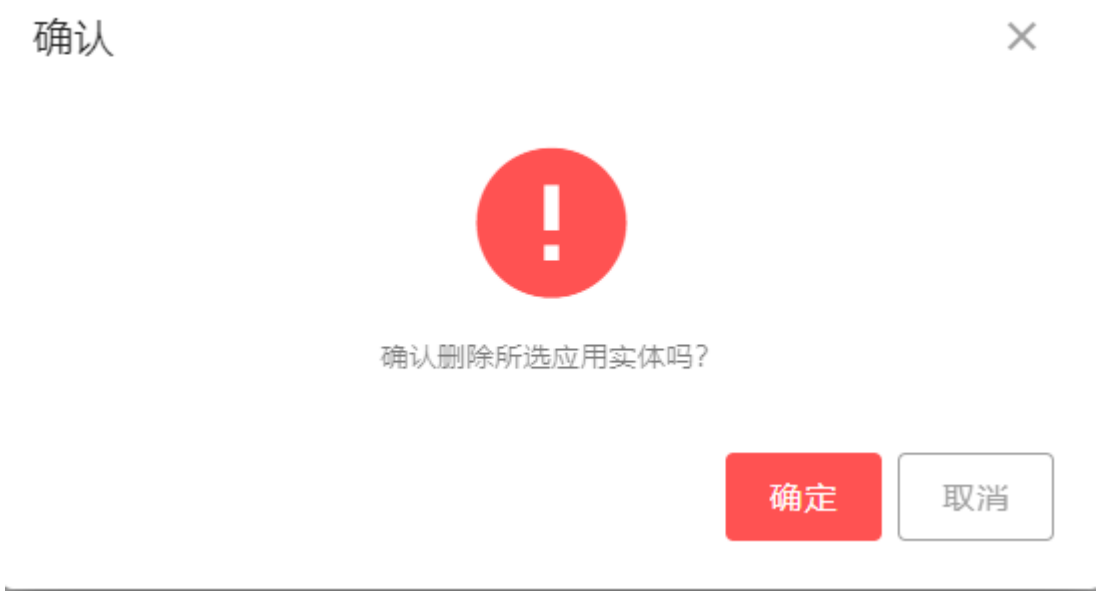

图3-20应用实体删除

点击“更多操作”里的“生成 P10 请求” ，弹出对话界面，如 0，输入部门、单位、城市、省份信息之后，点击【签名证书 P10 生成】、【加密证书 P10 生成】按钮，可以生成签名证书 P10 文件、加密证书 P10 文件并直接下载。

图3-21生成P10请求

点击“更多操作”里的导入证书，弹出对话界面，如 0，可上传签名证书文件、加密证书文件、加密密钥对文件（P12 格式），上述文件需要分别导入，其中密码是指 P12 密码，需要手动填写。**注：上传证书前需上传 CA 证书，具体可见 3.6.2CA 证书管理**

图3-22导入证书

点击“更多操作”里的“下载证书”，弹出证书下载窗口如 0，选择“下载签名证书”、“下载加密证书”，可下载应用实体证书。

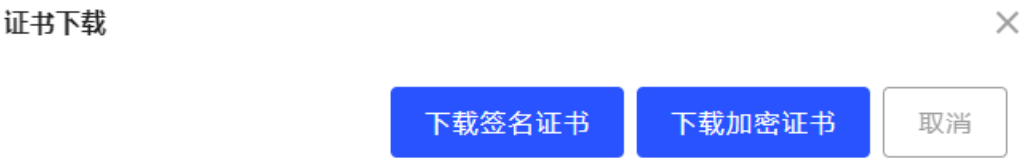

图3-23导入证书

点击“更多操作”里的“pdf 签章验签”，弹出证书 pdf 签章/验签窗口如 0，上传 pdf 文件即可进行签章验签。

图3-24Pdf签章验签

PDF 签章：选择需要签章的 PDF 文件，点击【PDF 签章】即可签章 PDF，如 0。签章完成之后，会自动生成一个签章后的 PDF 文件，如 0。

图3-25PDF签章

图3-26PDF签章完成

PDF 验签：选择自动生成的签章后的 PDF 文件，点击【PDF 验签】即可验签，如 0，并弹出验签成功结果，如 0。

图3-27PDF验签

图3-28PDF验签完成

应用实体删除：勾选应用实体所在行前“□”，可多选，点击【删除】，如 0，在弹出的对话框中点击确定后可将应用实体删除，弹出对话框如 0。

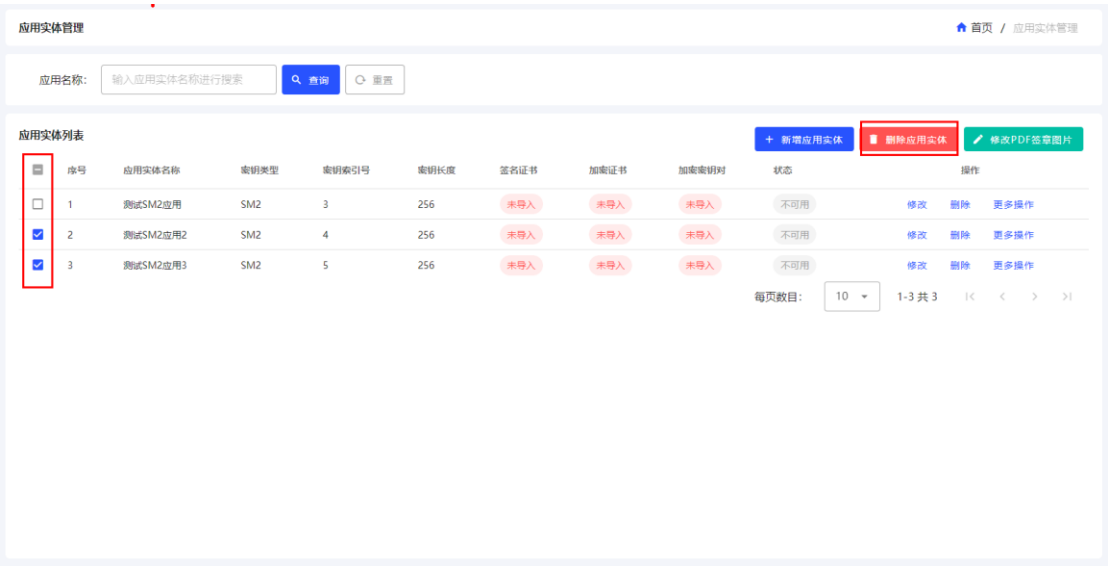

图3-29删除应用实体

图3-30删除对话框

修改PDF签章图片：主要功能是替换系统原有签章图片进行PDF签章，界面如0，点击按钮后弹窗如0.。可上传.bmp格式的图片作为pdf签章图片在签章后的pdf中进行展示。

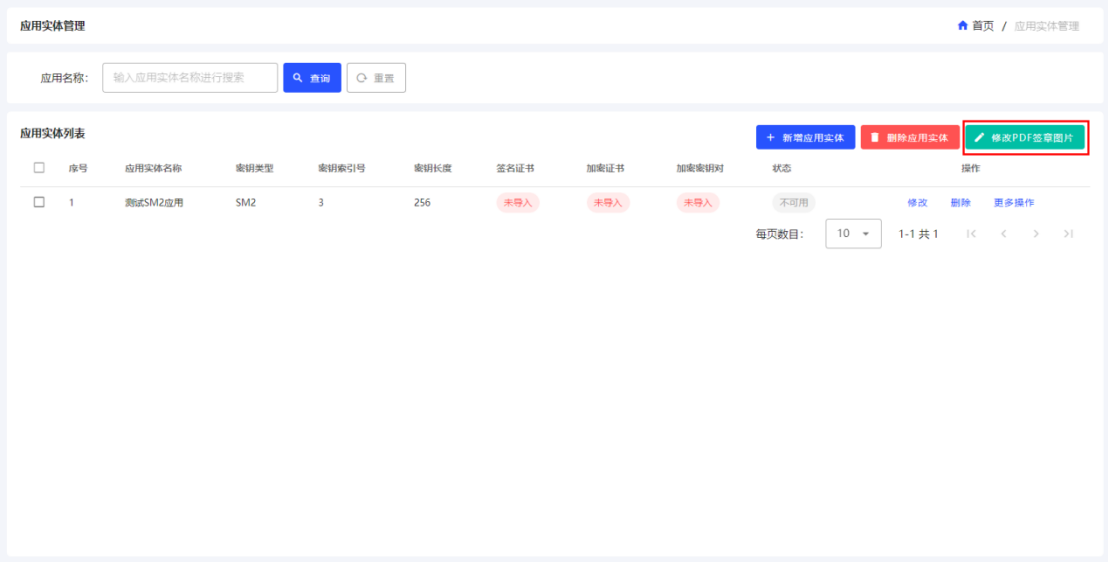

图3-31修改PDF签章图片

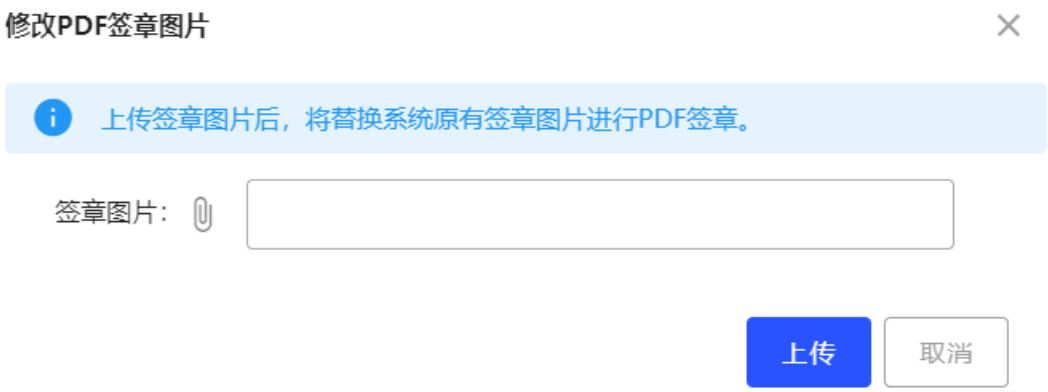

图3-32上传签章图片

3.2 数据备份恢复

选主要功能是实现对服务器数据的备份和恢复，界面内容如 0。

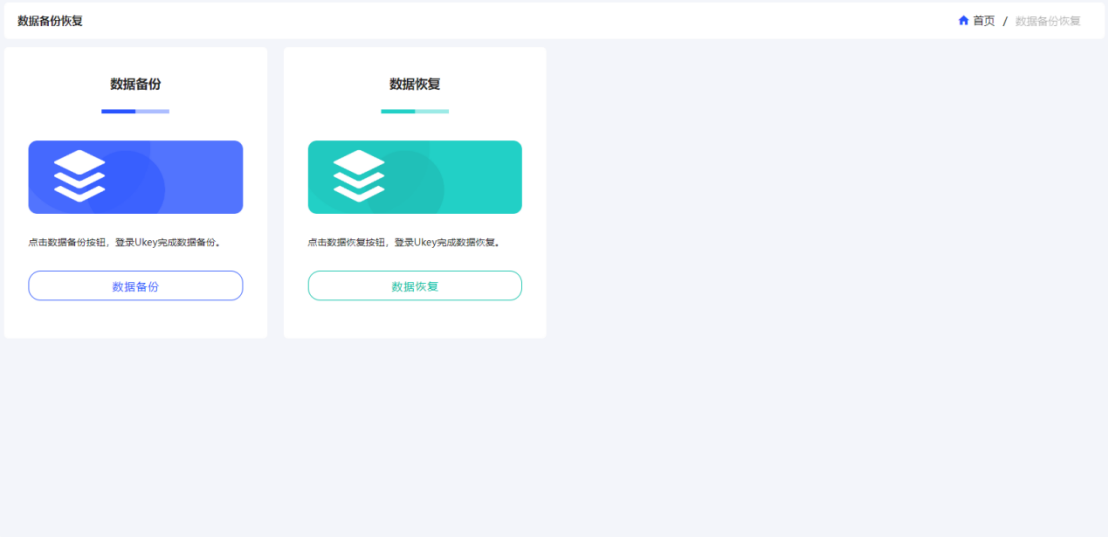

图3-33数据备份恢复

3.2.1 数据备份

点击“数据备份”按钮，在弹出窗先点击【开始备份】按钮。界面如 0。

图3-34开始备份

插入 UKey，点击【刷新】按钮后显示 UKey 序列号。界面如 0。

图3-35刷新

再点击【登录】按钮，在弹出框页面输入 UKEY 对应口令后，点击确定。界面如 0。

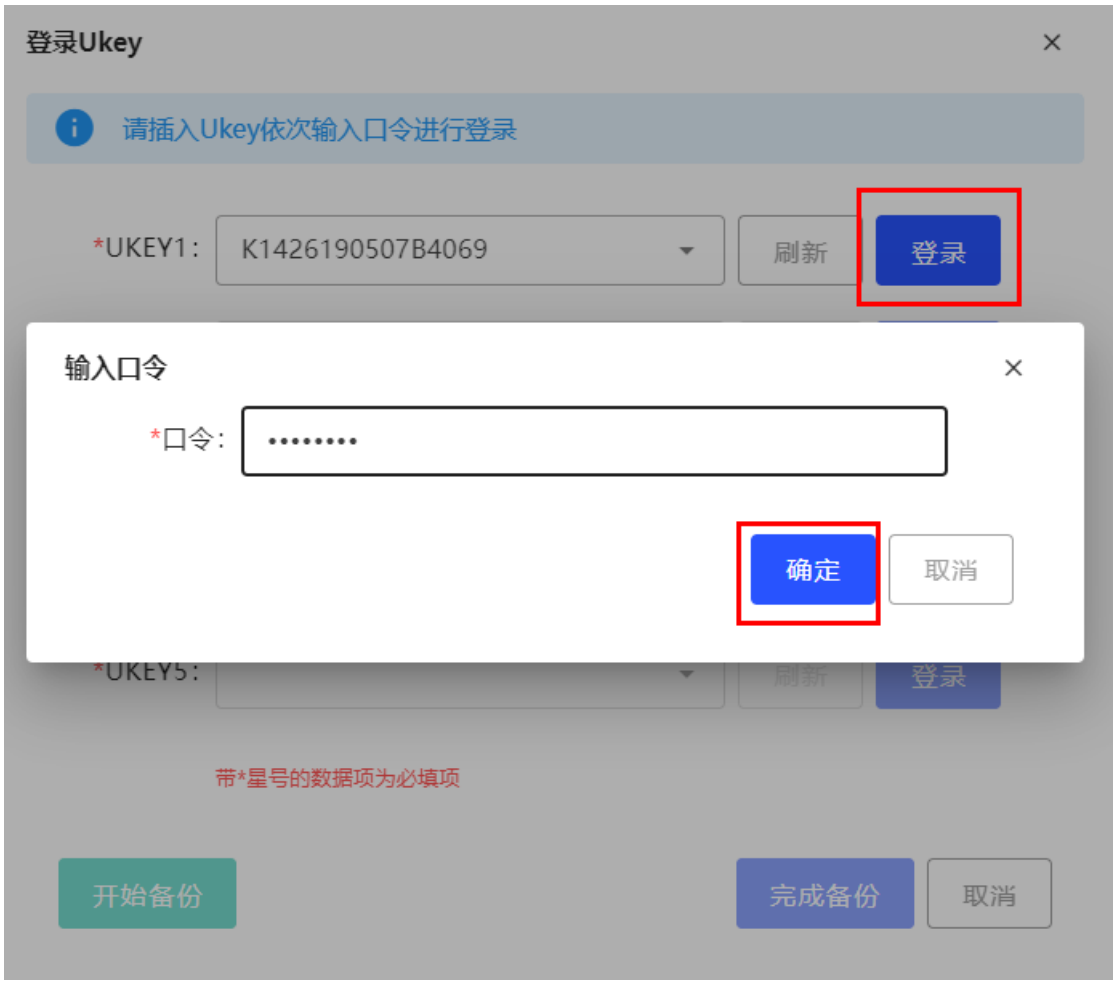

图3-36UKEY登录

顺着前面步骤依次把 5 个 Ukey 配置完成，备份密钥分割成 5 份，分别存储到 5 个 Ukey 中，完成全部密钥登录操作之后，点击【完成备份】按钮如 0，可将设备配置数据及密钥以密文形式下载到本地。界面如 0。

图3-37完成备份

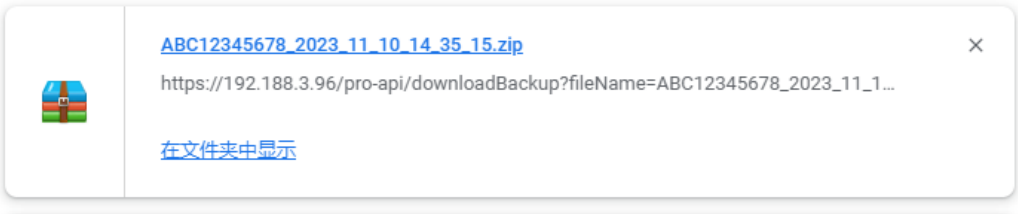

图3-38备份文件

3.2.2 **数据恢复**

点击【数据恢复】按钮，插入数据备份时所用到的 5 个 Ukey 中的任意 3 个 Ukey，界面如 0。

图3-39数据恢复

点击【登录】按钮，在弹出框页面输入 UKEY 对应口令后，点击确定。界面如 0。

图3-40数据恢复登录

顺着前面步骤依次把 3 个 Ukey 配置完成之后，版本号则自动填入下拉列表中，选择需要恢复的版本号，并选择对应版本号的备份文件。界面如 0。

图3-41选择版本

点击【开始恢复】按钮，弹出确认提示框，如图 3-42。

图3-42恢复确认

点击【确定】后开始恢复，如 0，恢复完成后提示重启设备后生效，如 0。

图3-43正在恢复

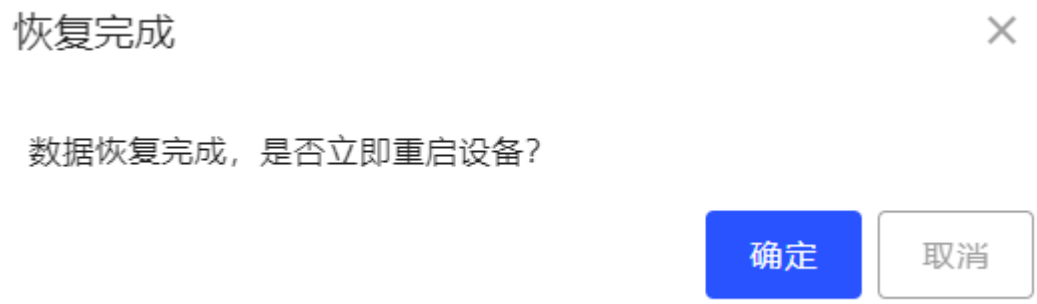

图3-44恢复完成

3.3 双机热备管理

在选择双机热备功能状态开启模式下，才可配置双机热备功能；选中“启动双机热备”选项，选择主服务设备网口，输入主服务 IP、另一台热备设备 IP 地址、虚拟路由

ID，点击“保存配置”，完成此设备的双机热备配置，界面如 0。要真正实现双机热备功能，还需要在另一台签名验签服务器上按上述配置完成双机热备配置，同时保证双台设备间网络可达。**注意：做双机热备的两台设备 IP 地址必须在同一网段，虚拟路由 ID 必须相同，且同一网段下如果存在多组双机热备，每组的虚拟路由 ID 必须互不相同，建议使用主服务 ip 最后一组数作为虚拟路由 ID 可保证不与同网段其他组热备冲突。**配置双机热备前提条件：必须保证创建并使用相同的 Ukey 操作，同时建议分别初始化两台设备，保证双机热备时两台设备数据一致。**注：主、备双机热备配置完成之后，此时并未数据同步，若实现数据同步两台设备需依次点击“开启数据同步”按钮。当开启后会有主备状态的区分，双机热备功能状态分别为：已开启，当前为主机；已开启，当前为备机，如 0。**开启过程如 0。

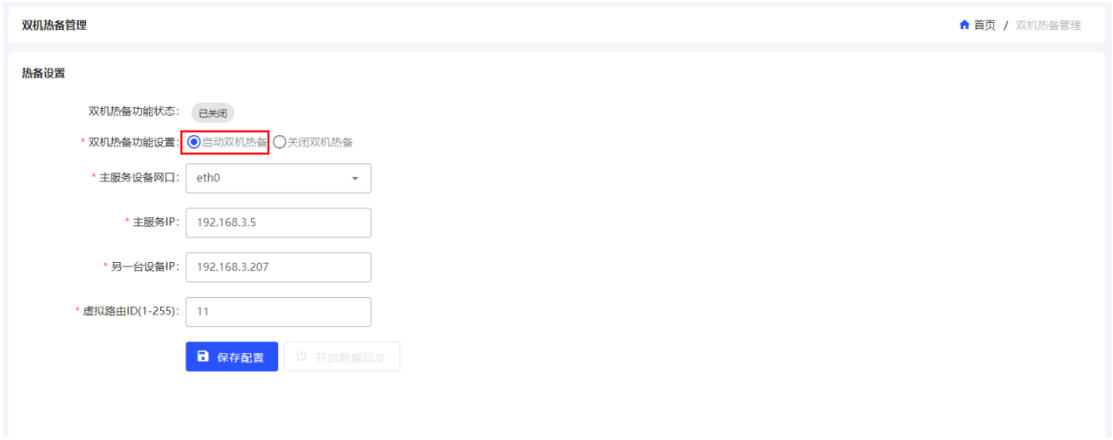

图3-45双机热备

图3-46开启数据同步

图3-47数据同步开启成功

注意：数据同步开启后请访问主服务 IP 进行操作，请勿再访问子服务 IP 操作（详情请看“常见问题及解答”）。

关闭双机热备时选择“关闭双机热备”，再点击保存配置，如 0 所示。

注意：关闭双机热备时，需访问两台设备的子服务IP，分别进行关闭操作，不可直接在主服务IP上进行关闭。若已开启数据同步，关闭双机热备后需手动重启才可继续操作设备。

图3-48关闭双机热备

3.4 用户管理

3.4.1 系统用户管理

系统用户管理显示当前系统所有用户的信息，具体显示内容包括用户角色、对应 UKEY 的序号、登陆状态，以及新建用户、设置用户口令过期天数、删除用户、修改口

令。界面如 0。

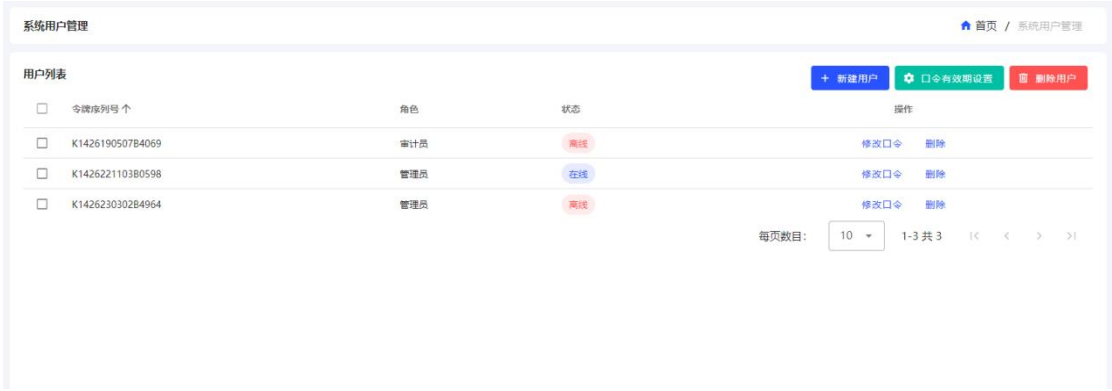

图3-49系统用户管理

点击“新建用户”按钮，选择添加的用户角色(管理员、操作员或审计员)，插入 Ukey，若未识别 Ukey 信息，可点击“刷新”按钮，输入令牌口令（默认口令 12345678），以及新口令和确认新口令（新口令由 8-16 位数字、大小写字母或特殊字符的三种或三种以上组合），点击“确定”，即可完成新增管理员、操作员或审计员添加操作，操作界面如 0。注：新口令与原令牌口令不能相同。

图3-50新建用户

点击“口令有效期设置”可设置用户口令过期天数。在用户口令过期天数输入天数，点击【确定】完成用户口令过期天数配置（设置为 0 时关闭用户口令过期提醒）。如 0。

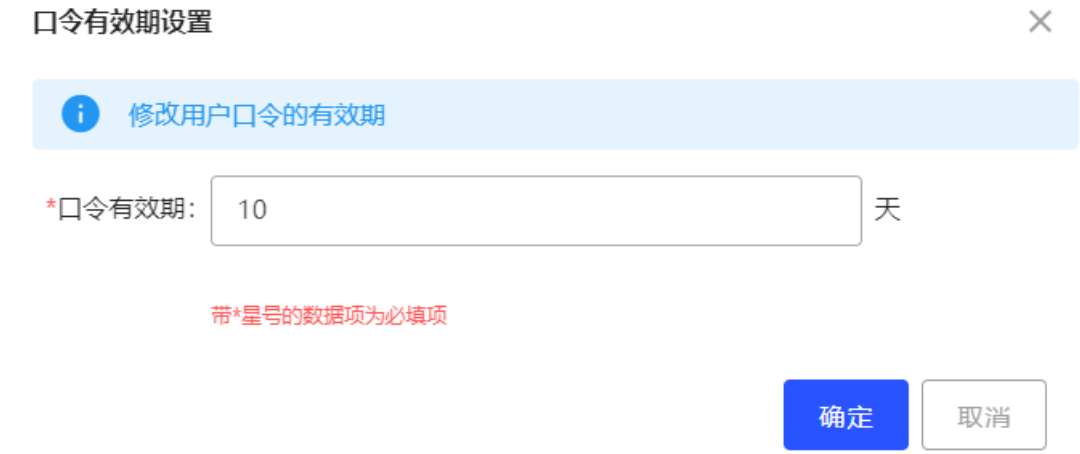

图3-51口令有效期设置

勾选用户所在行前的“□”，点击“删除用户”如 0，可将该用户删除。弹出框如 0。

图3-52选择用户

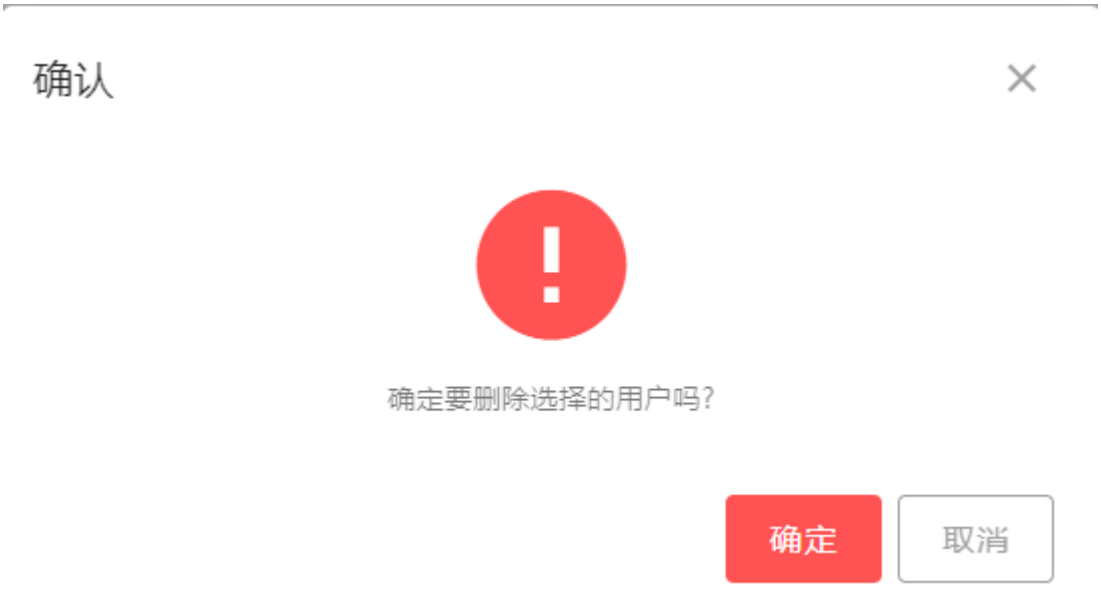

图3-53用户删除

点击用户列表中的“修改口令”，可修改对应用户的口令（需插入该用户绑定的 Ukey），新口令不能和原口令相同且新口令和确认新口令必须一致，输入原口令、新口令以及确认新口令后（口令由 8-16 位数字、大小写字母或特殊字符的三种或三种以上组合），点击【确定】，验证通过后，即可完成用户 Ukey 口令的修改，界面如 0。

图3-54修改口令

点击用户列表中的“删除” 如 0，弹出提示框后，点击确定可单独删除对应的用户信息，如 0。

图3-55删除用户

图3-56删除提示框

3.4.2 restful用户管理

restful 用户管理显示当前系统所有 restful 用户的信息，具体显示内容包括用户名和备注信息，以及新建用户、删除用户、修改口令和用户搜索功能。如 0。

图3-57restful用户管理

点击“新建用户”按钮，输入用户名、口令和确认口令后，点击“确定”，即可完成新增 restful 用户操作，用户名只能由 4 到 16 位（字母，数字，下划线，减号）组成，操作界面如图 3-57 图 3-58。

图3-58新增restful用户

勾选用户所在行前的“□”，点击“删除用户”如**错误!未找到引用源。**，可将该用户删除。弹出框如 0。

图3-59选择用户

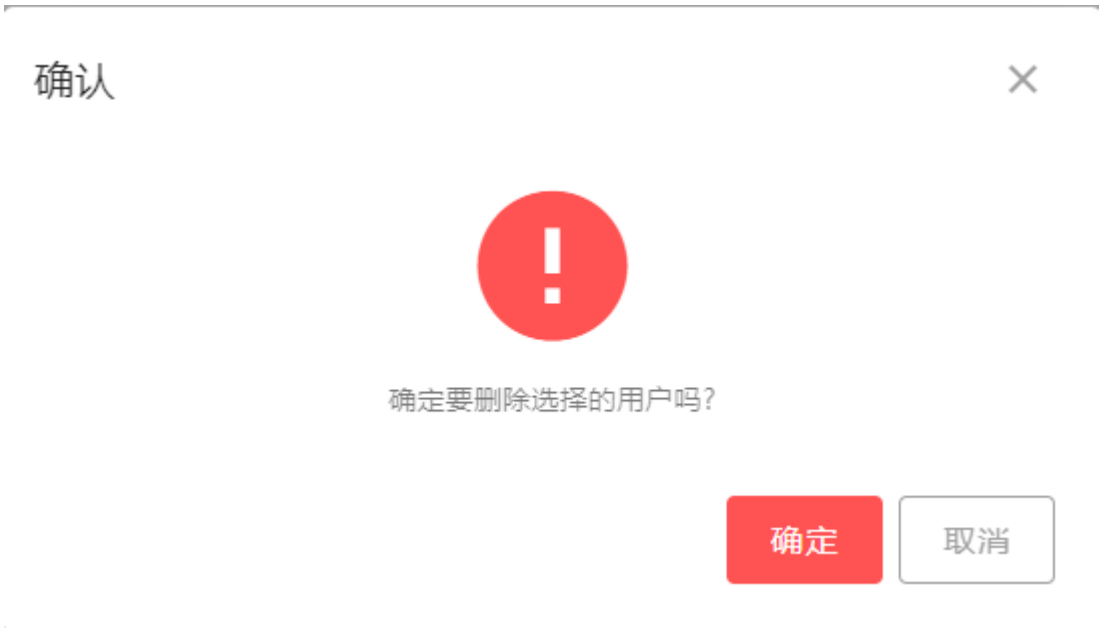

图3-60用户删除

点击用户列表中的“修改口令”，可修改对应用户的口令，输入新口令以及确认新口令后，点击【确定】，即可完成 restful 用户口令的修改，界面如 0。

图3-61修改口令

点击用户列表中的“删除” 如 0，弹出提示框后，点击确定可单独删除对应的用

户信息，如 0。

图3-62删除用户

图3-63删除提示框

搜索框中“用户名”和“备注”支持模糊查询，可按条件查询出对应的用户信息，清空按钮用于重置查询条件，界面如 0。

图3-64按条件搜索

3.5 设备管理

3.5.1 初始化

初始化设备需要先开启初始化功能，再点击【初始化设备】，才可进行设备初始化。点击【开启初始化功能】，可以开启初始化设备功能；点击【关闭初始化功能】按钮，可以关闭初始化设备功能，界面如 0。**注：初始化会清除设备所有的用户、数据、配置和密钥，初始化前请做好备份。**

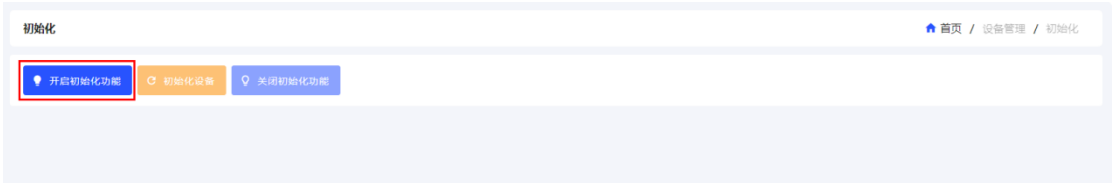

图3-65初始化设备

点击【开启初始化功能】后，【初始化设备】按钮为可点击状态，如 0，然后就可以通过点击【初始化设备】进行设备初始化。

图3-66初始化设备

点击【初始化设备】后会弹出确认窗口，如 0。点击确定后进行初始化，初始化完成后弹出初始化完成提示，点击确定回到登录页面。如 0，初始化过程大约需要一分钟。

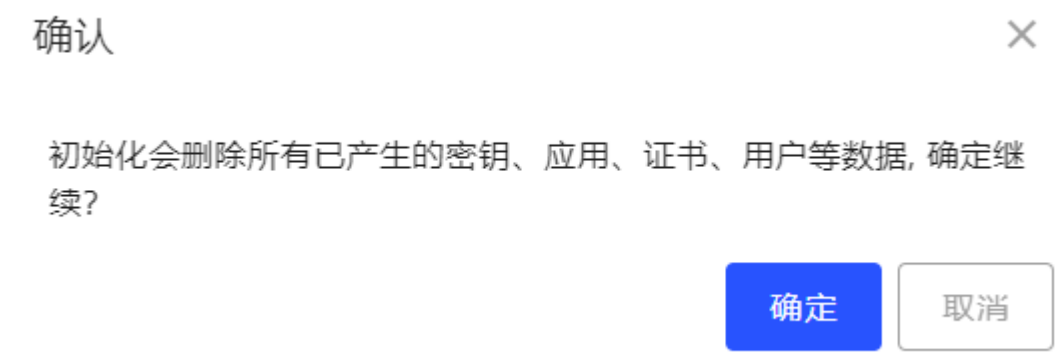

图3-67初始化确认

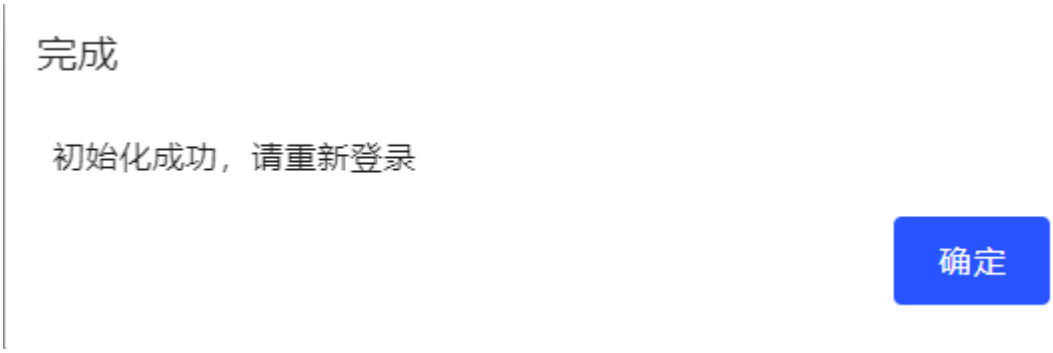

图3-68初始化完成

若禁用点击【初始化设备】，可点击【关闭初始化设备】如 0 ，点击【关闭初始化功能】后，【初始化设备】按钮为禁用状态，如 0。

图3-69关闭初始化功能

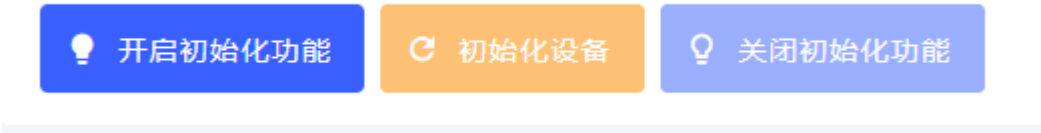

图3-70关闭初始化功能后

3.5.2 系统升级

系统升级页面可以使用升级包升级系统，界面如 0。点击【系统升级】，在弹出框中选择升级文件，点击“开始升级”，进行系统升级，界面如 0。

图3-71系统升级

图3-72升级文件

3.5.3 设备信息

设备信息显示生产厂商信息、硬件版本信息、软件版本信息、产品序列号、设备名称信息。界面如 0。

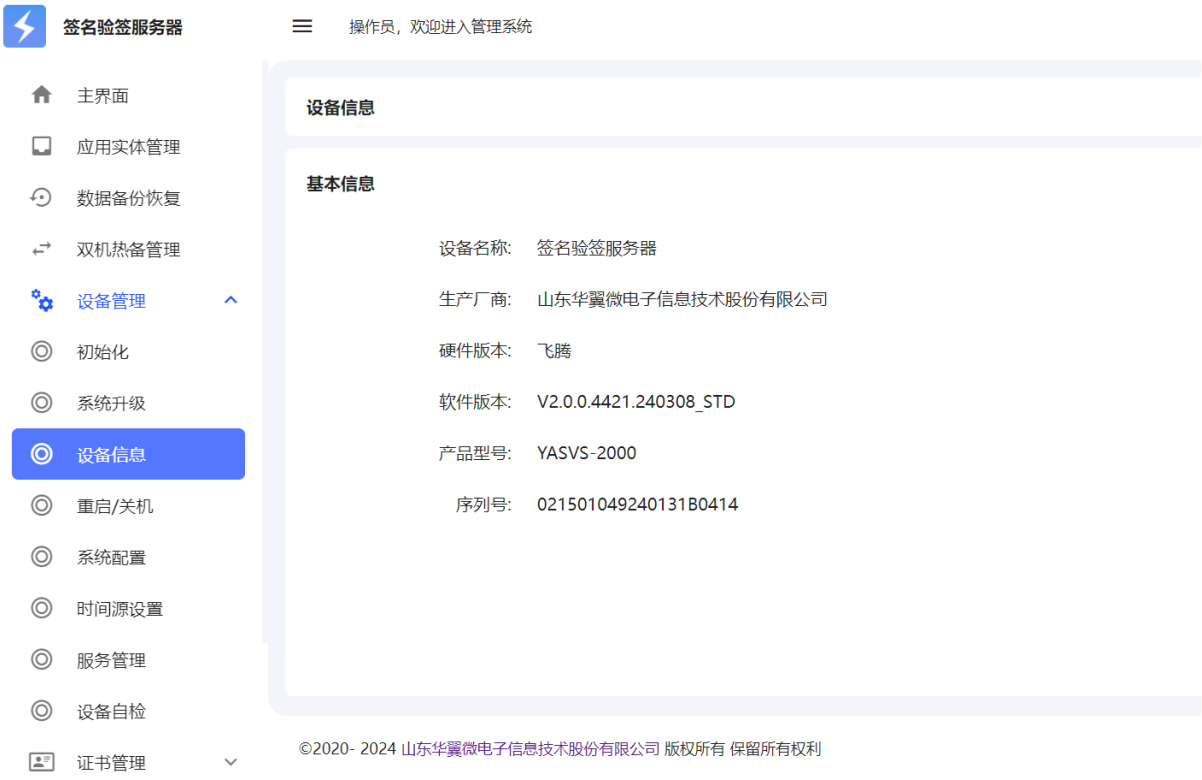

图3-73设备信息

3.5.4 重启/关机

提供在重启/关机页面手动重启和关机的功能，界面如 0。

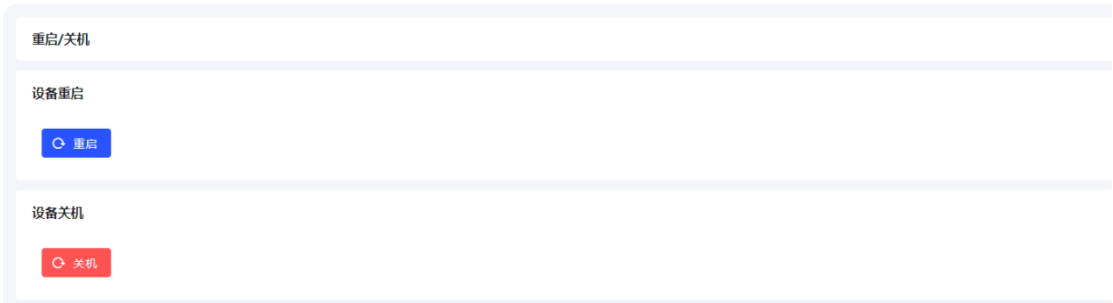

图3-74重启/关机界面

点击“重启”，会弹出“设备正在重启，稍后请重新登录!”提示信息框，如 0。点击确定后，自动跳转至登录页面，待重启成功之后，用户可刷新登录页面重新登录。点击“关机”后，会弹出“设备正在关机，无法正常使用!”提示信息框，如 0。点击确定后，自动退出登录。 **注：1、用户可不断刷新登录页面确认是否重启成功。2、为避免浏览器缓存，在登录之前可刷新登录页面，确定重启成功后，再登录。**

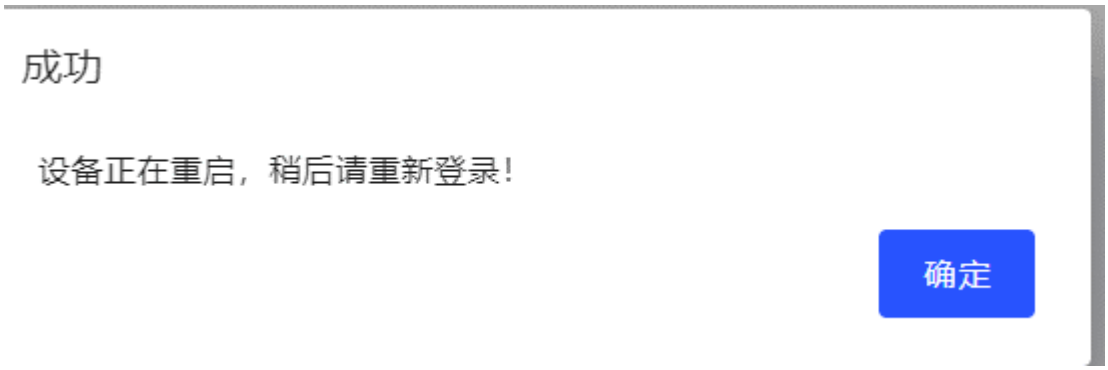

图3-75重启提示

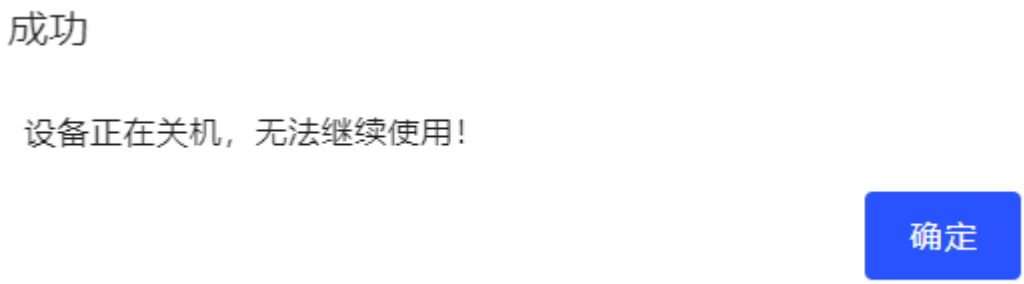

图3-76关机提示

3.5.5 系统配置

系统配置页面包含“网络配置”、“路由配置”、“白名单配置”以及“时间配置”功能。界面如 0。

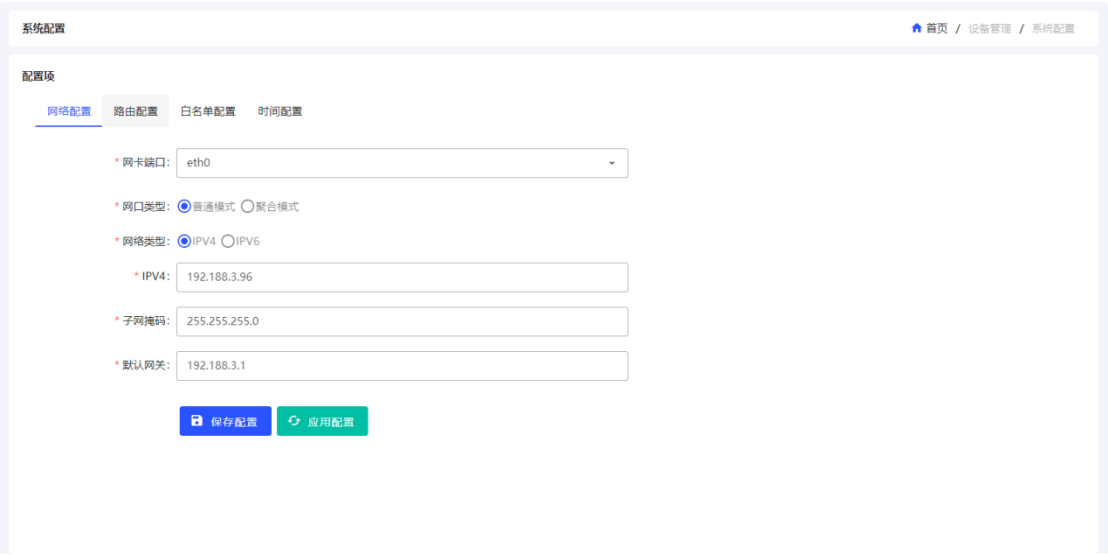

图3-77系统配置

网络配置：网络配置可以配置设备的网络参数。选择网卡端口、网口模式、网络类型，输入 IP 地址、子网掩码、网关信息，点击【保存】，即可完成网络配置操作，IPV4 界面如 0，IPV6 界面如 0。网口模式选择聚合模式，可以将所有配置成聚合模式的网口聚合为一个 IP，界面如 0。

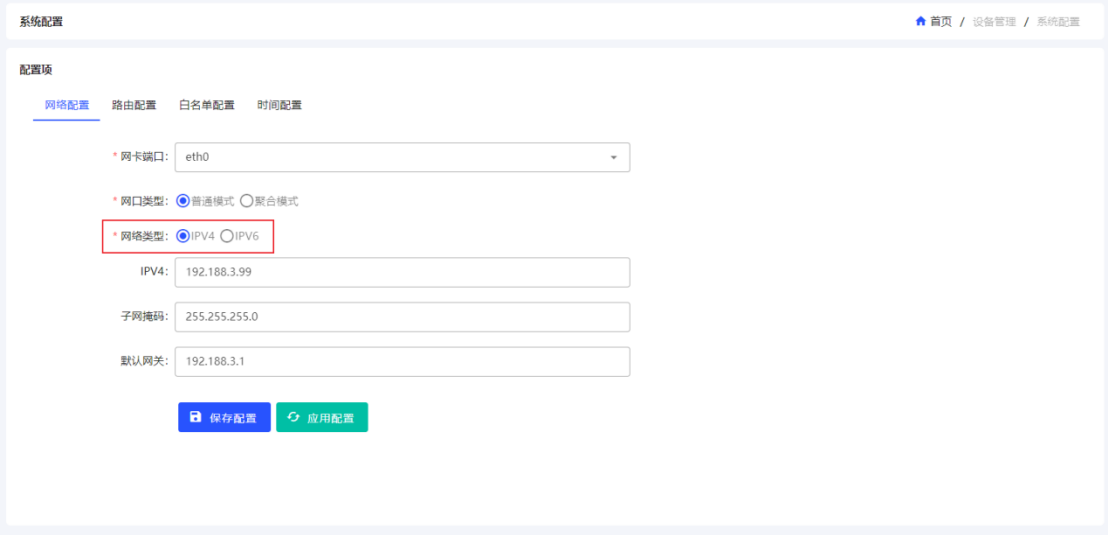

图3-78IPV4网络设置

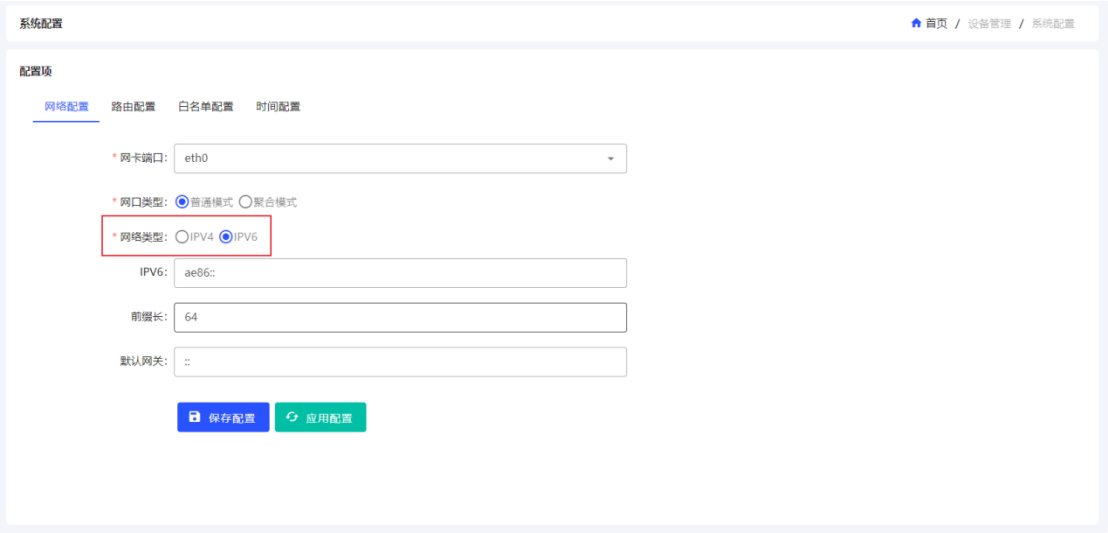

图3-79IPV6网络设置

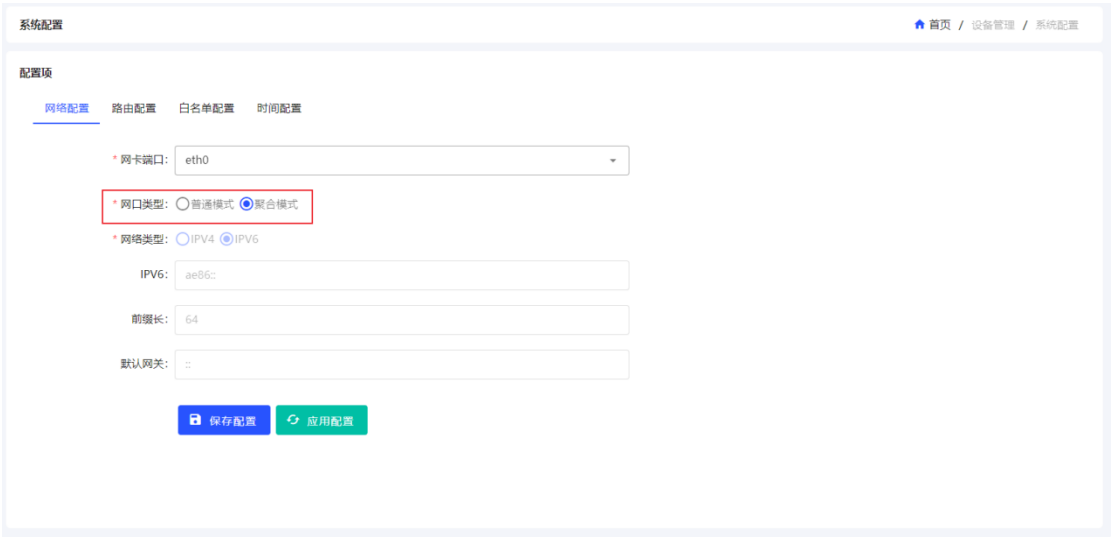

图3-80聚合模式

配置聚合模式后，网卡端口新增“bond”选项，选择bond端口后可配置聚合模式以及聚合IP等信息。其中聚合模式包括0~6七种模式分别是：0平衡轮循策略、1主-备份策略、2平衡策略、3广播策略、4动态链接聚合、5适配器传输负载均衡、6适配器适应性负载均衡，如0。。**注：除模式1以外其余模式需要路由器支持。**

图3-81聚合模式

网络配置需要重启设备后才会生效。如0。保存配置成功后，点击【应用配置】则

无需重启设备，会使当前网络配置立即生效。如0。**注：请确认不同网口不在同一网段内，否则可能导致网口的网络无法使用。**

图3-82重启提示

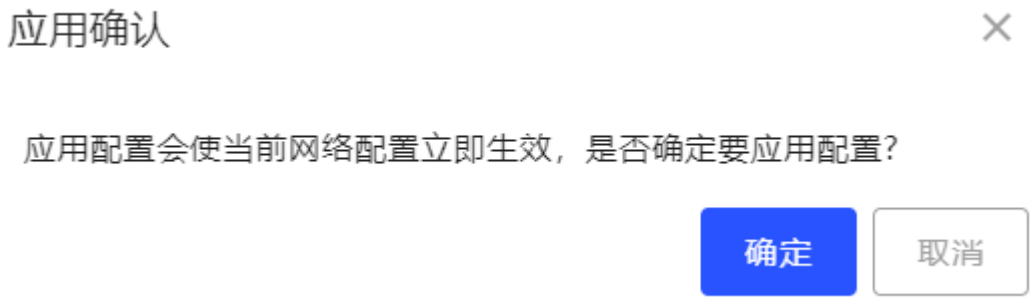

图3-83应用配置

路由配置：路由地址的 IP 配置，需要配置 IP 地址、子网掩码和网关。如 0。

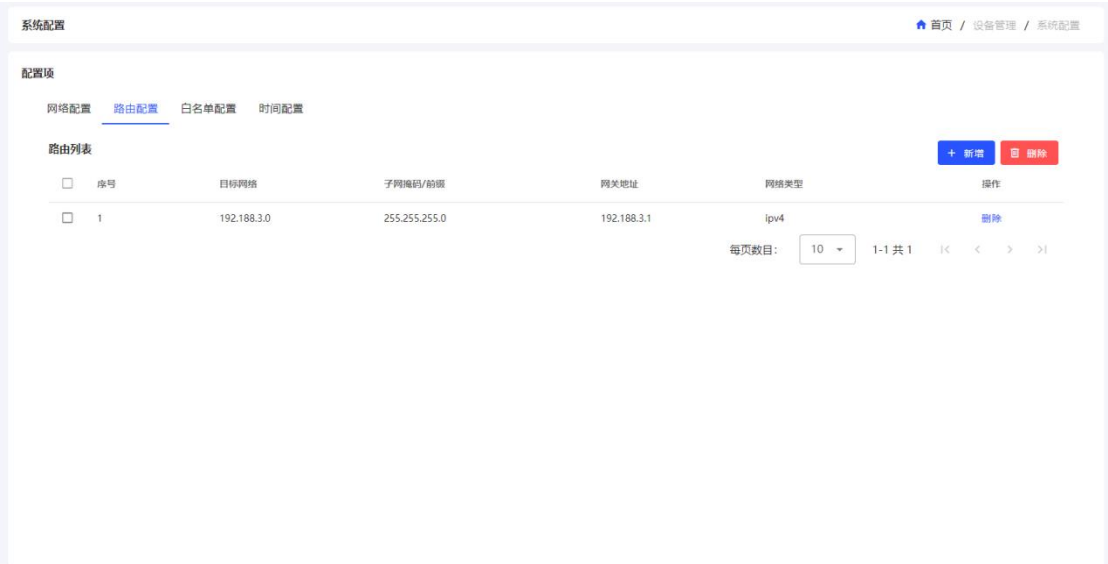

图3-84路由配置页面

点击【新增】按钮，在弹出框中选择网络类型 IPV4 或 IPV6，IPV4：输入目标网络、子网掩码和网关地址；IPV6：输入目标网络、前缀长度和网关地址。点击【确定】，可新增路由，如 0。

图3-85IPV4/IPV6路由配置

勾选目标网络前的“□”，可多选，点击【删除】即可删除选中路由地址，或点击列表操作列的“删除”如 0。弹出删除确认框，如 0。点击确定完成删除。

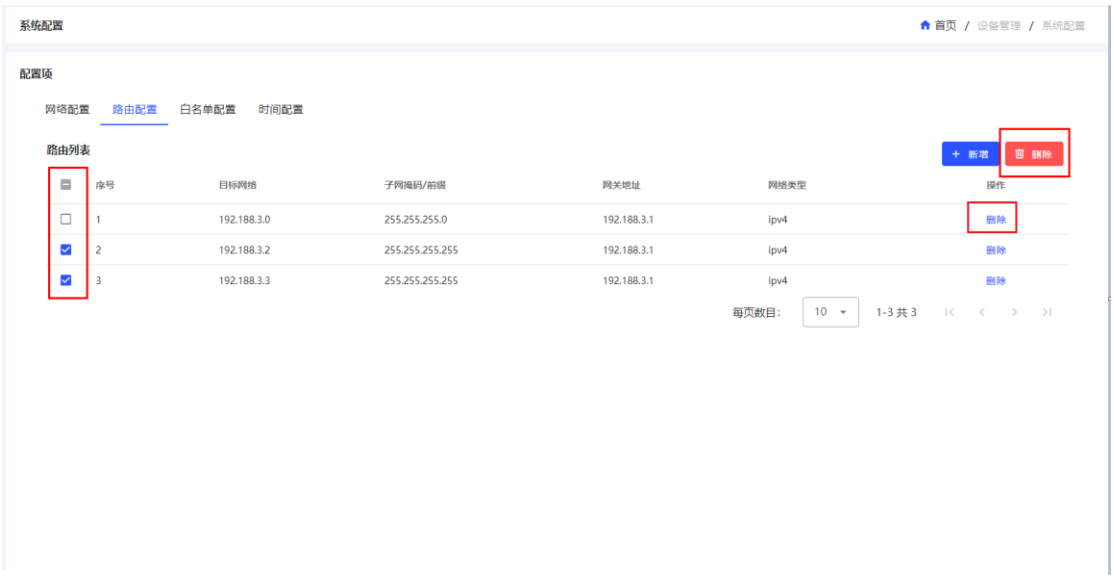

图3-86删除路由

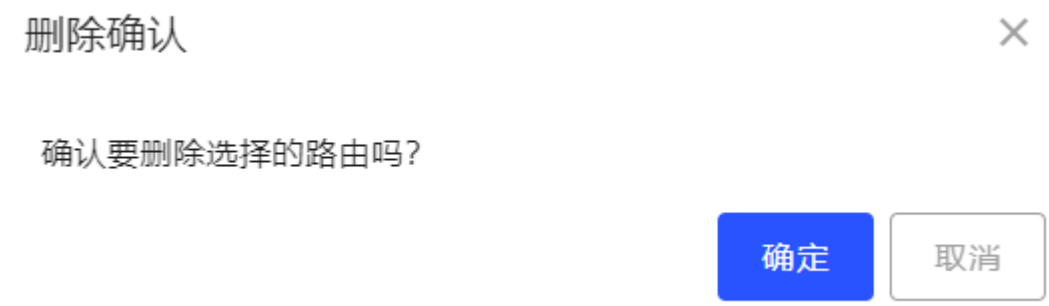

图3-87删除确认

白名单配置：白名单的 IP 配置可以是 IP 网段或 IP 地址，配置 IP 之后，只允许白名单中的设备访问服务器，白名单之外的设备不允许访问，如 0。（白名单列表为空时，白名单功能关闭）

图3-88白名单配置

点击【新增】，在 IP 栏输入 IP 或者 IP 段，可以在备注栏输入白名单备注，点击【确定】，可新增白名单，如 0。

图3-89新增白名单

勾选白名单前的“□”，点击【删除】即可删除选中白名单，或通过点击列表中操作列的“删除”，进行单个白名单的删除操作如 0。当删除的不是最后一个白名单时，提示如 0。当最后一个白名单被删除时提示如 0。

图3-90删除白名单

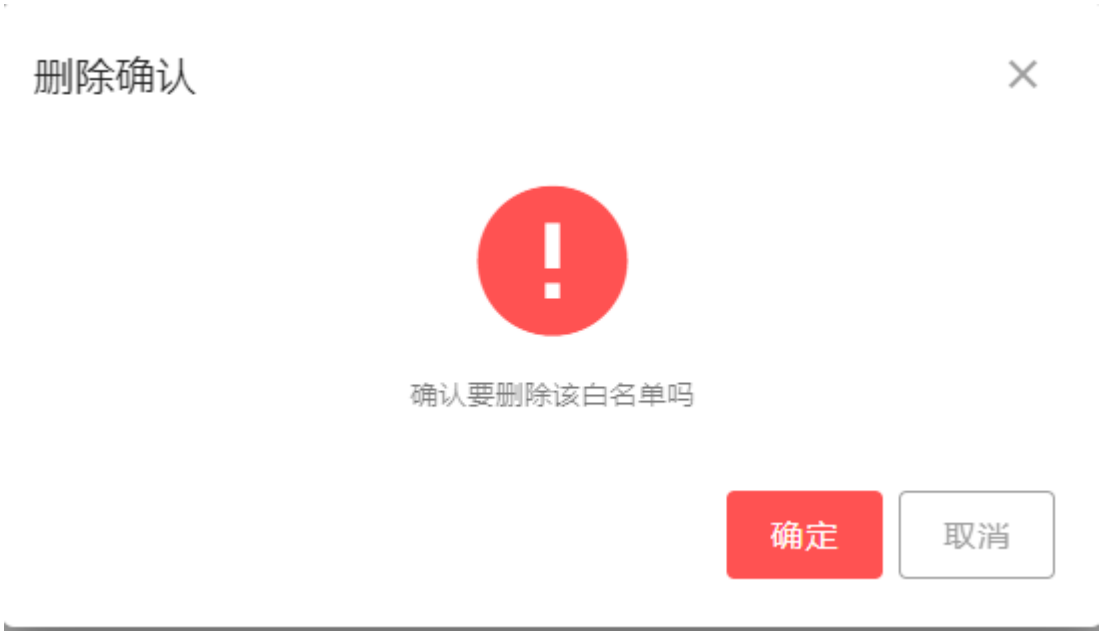

图3-91删除白名单

图3-92删除全部白名单

时间配置：时间可以配置当前系统时间，在设置系统时间输入栏输入系统时间，点击【设置】，可修改系统当前时间。界面如 0。

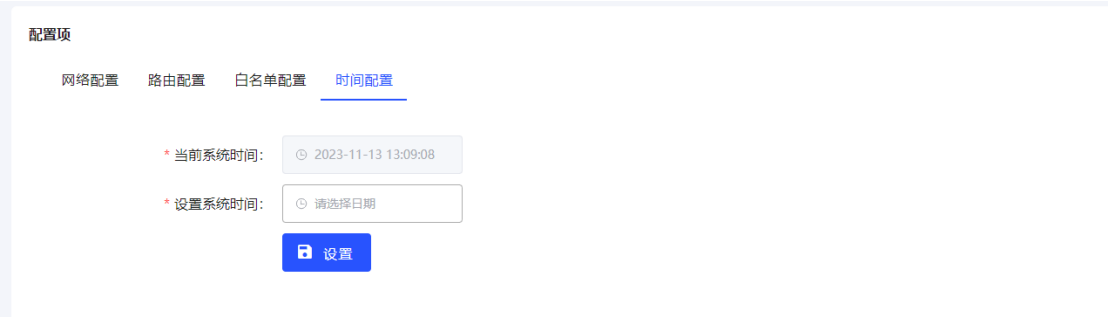

图3-93时间配置

3.5.6 时间源设置

时间源配置包括 NTP 对时设置、北斗对时设置。界面如 0。**注：设备分为带授时卡和不带授时卡两种版本，只有带授时卡的设备才会显示“北斗对时设置”，否则不显示。**

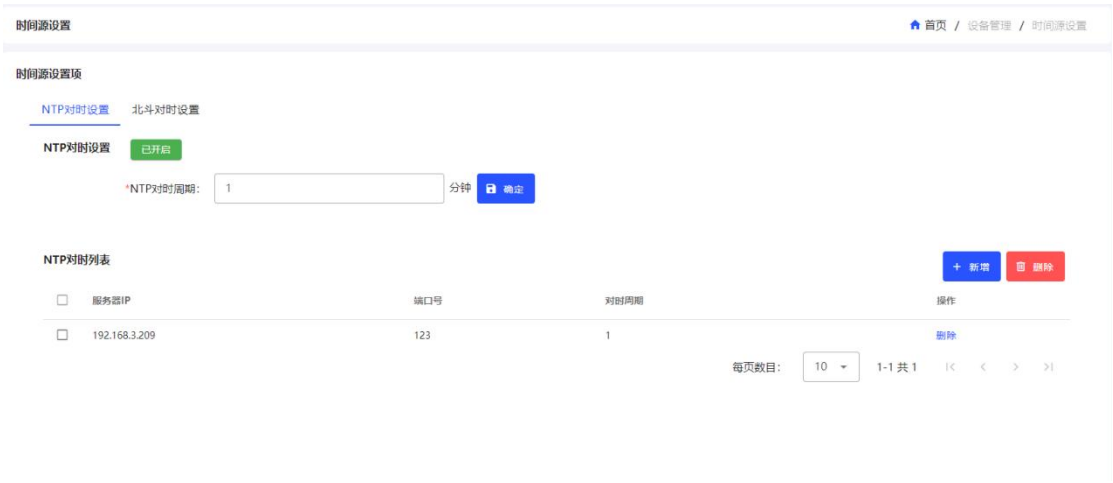

图3-94时间源配置

NTP 对时设置：NTP 对时列表内容为空时，代表未配置 NTP 对时，此时 NTP 对时设置显示为“已关闭”状态，如 0。

图3-95已关闭

点击“新增”按钮，弹出对话框如 0，输入 NTP 服务器 IP 地址、点击“确定”，即可开启 NTP 对时设置，自动与 NTP 服务器进行时间同步。如 0 所示。

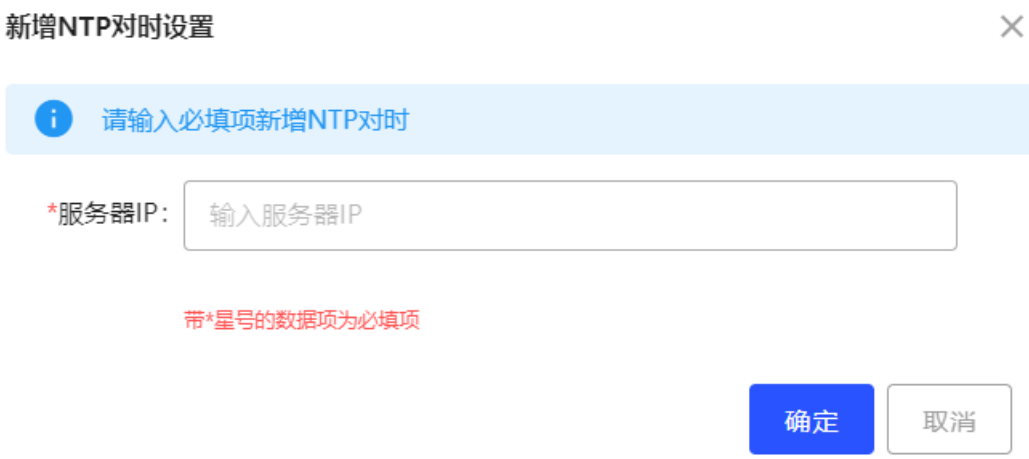

图3-96对时设置

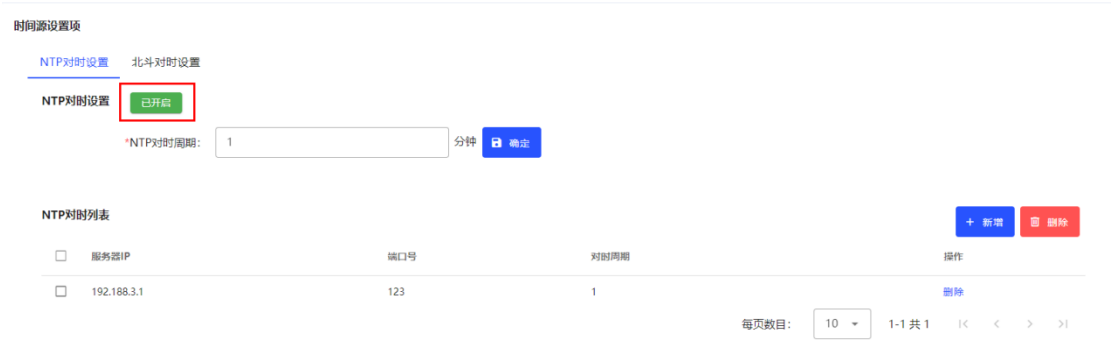

图3-97对时开启

NTP 对时周期输入框可修改 NTP 对时周期设置，点击“确定”，即可修改所有服务器 IP 的对时周期。如 0 所示。

图3-98对时周期

北斗对时设置：点击“北斗对时设置”标签切换到北斗对时设置页面，如 0 所示。输入北斗定时对时周期，点击“开启”，即可自动与北斗卫星进行对时，时间同步。点击“关闭”，即可关闭北斗对时服务。

图3-99北斗对时设置

3.5.7 服务管理

服务管理页面可配置 SSH、国密 SSH、国密 FTP、国密 SSL、SNMP 服务的开启和关闭。以及 SNMP 团体字的功能。如 0。

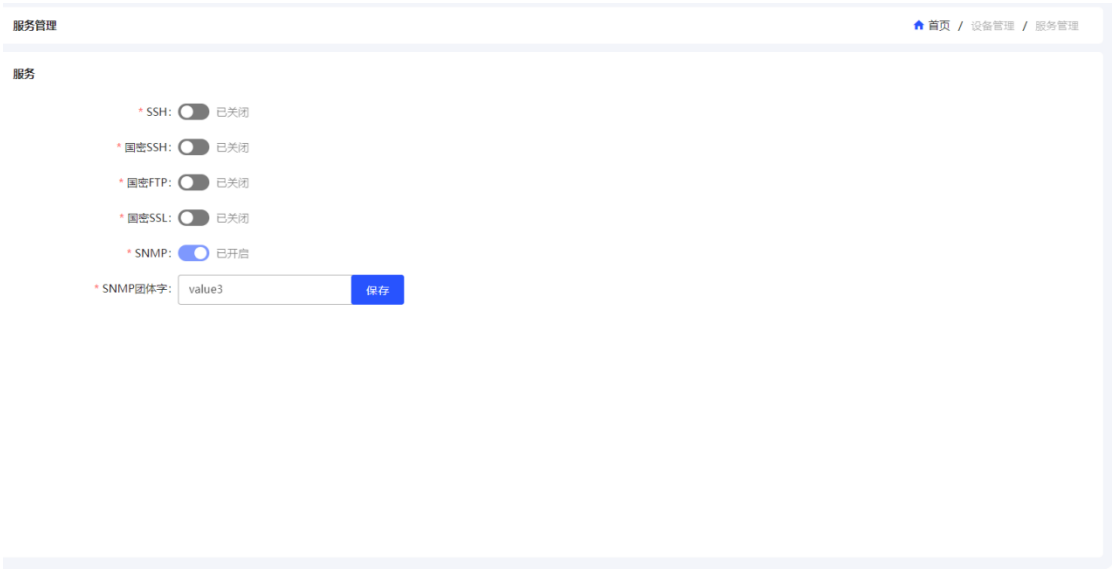

图3-100服务管理

点击按钮即可切换对应服务的开启和关闭状态。如 0。

图3-101关闭/开启状态

点击【保存】即可保存 SNMP 团体名并生效，页面上显示修改后的 SNMP 团体名，如 0。**注：从安全角度考虑，尽量避免将 snmp 的团体字修改为 public 这一默认值。**

图3-102SNMP团体字

3.5.8 设备自检

设备自检页面中可以设置设备定时自检时间，设置时间后，每天到达设置时间后，

会自动进行自检。手动填写时间的时分，点击设置按钮进行设置，如 0。

图3-103设备自检

页面中显示自检结果，可以点击手动自检按钮手动执行一次自检，如 0。

图3-104手动自检

3.6 证书管理

3.6.1 证书查询设置

证书查询设置包括 OCSP 在线查询、CRL 自动更新两种方式的设置。选择“OCSP 在线查询”，输入 OCSP URL 地址、点击“保存”，完成 OCSP 在线查询方式设置。界面如 0。

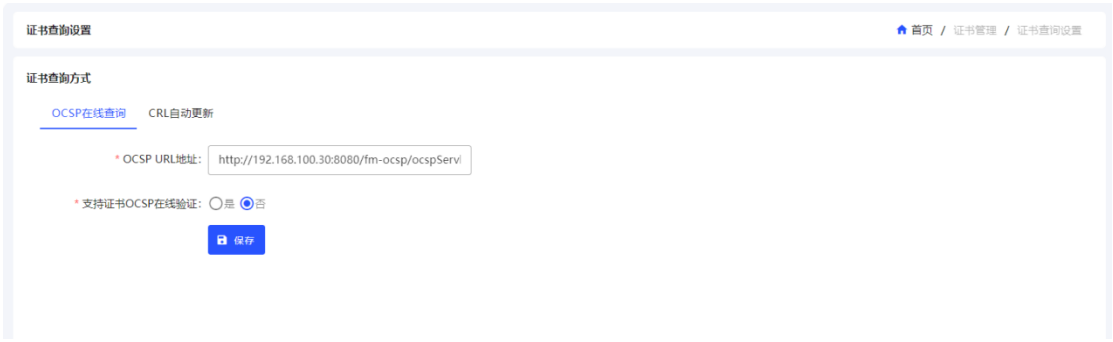

图3-105OCSP在线查询

选择“CRL 自动更新”，输入 LDAP 服务器的 URL 地址、基本 DN 信息，选择是否自动更新，点击“保存”，完成 CRL 自动更新设置。界面如 0。

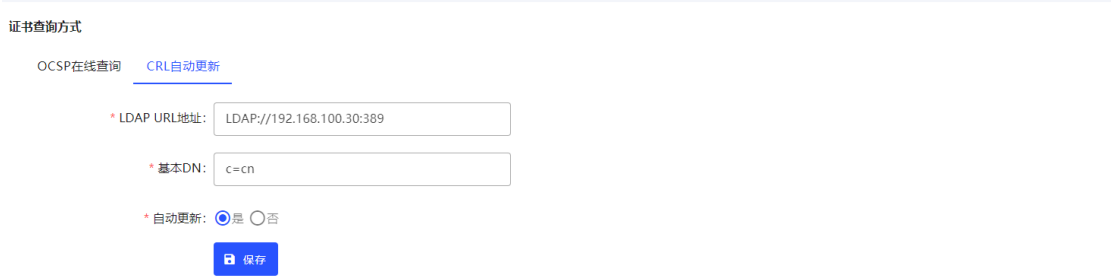

图3-106CRL自动更新

3.6.2 CA证书管理

CA 证书管理包括 CA 证书、证书链的导入、证书信息展示和证书删除，支持多 CA 证书的导入。界面如 0。

图3-107CA证书管理

点击【导入】，在弹出框中选择证书类型，以及证书或证书链文件，点击“导入”就可以导入 CA 证书或证书链。如 0 所示。

图3-108导入CA证书

勾选证书所在行前的“□”，点击【删除】，或者点击 CA 证书列表中操作列的“删除，”可以删除所选证书的信息。如 0。

图3-109删除CA证书

3.6.3 CRL管理

CRL 管理包括 CRL 的导入、显示与删除功能，如 0。点击“CRL 导入”选择需要上传的 CRL 文件，再点击“导入”即可上传 CRL 文件。如 0。

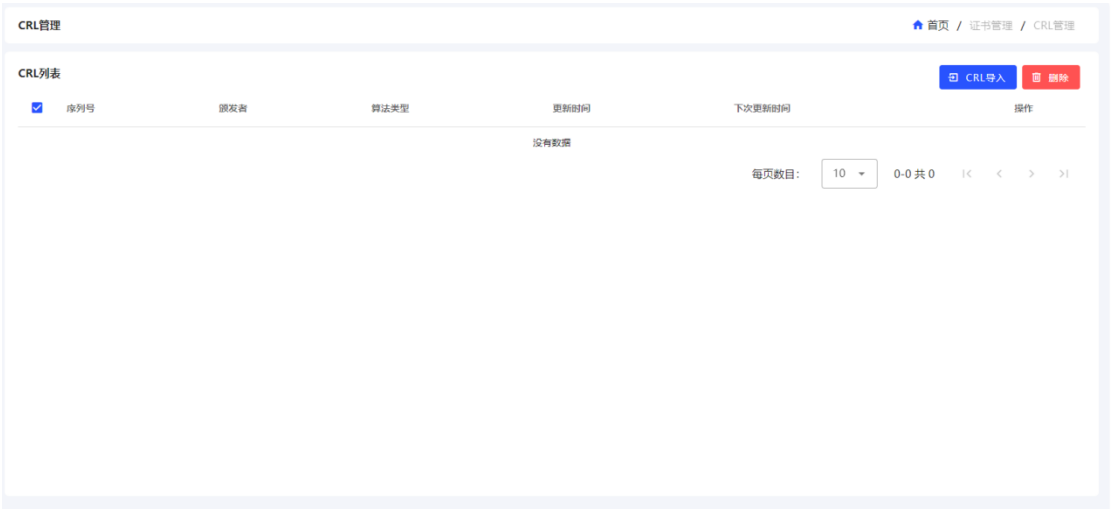

图3-110CRL管理

图3-111导入CRL

勾选 CRL 所在行前的“□”，点击右上“删除”按钮，或者点击 CRL 列表里操作列的删除，即可将选中的 CRL 删除。界面如 0。

图3-112CRL删除

3.6.4 用户证书管理

用户证书管理包括用户签名证书、加密证书的导入、用户证书查询和用户证书删除功能，界面如 0。

图3-113用户证书管理

点击【证书导入】，选择证书类型和用户证书文件就可以导入用户证书，如 0。

图3-114导入用户证书

输入对应的“主题”，选择证书状态，点击【搜索】按钮显示所对应的信息，【清空】可以清除输入的内容。如 0。

图3-115用户证书搜索

勾选证书所在行前的“□”，可多选，点击右上角【删除】按钮可以删除所选证书的信息，或点击用户证书列表中操作列的删除，可以删除对应证书。如 0，点击【删除】，提示是否删除的确认框，如 0。

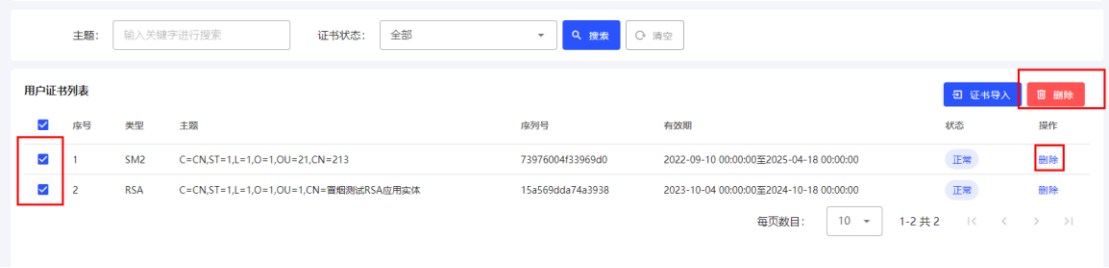

图3-116用户证书搜索

图3-117证书删除确认框

3.6.5 设备证书管理

设备证书管理包括设备密钥的 P10 文件生成及设备证书的导入，其中设备密钥固定密钥索引号为 0，设备证书包括为设备签名证书和设备加密密钥（P12 格式）的导入。如 0。

图3-118设备证书管理

点击【管理密钥生成】按钮，在弹出框中展示管理密钥的状态（管理密钥默认为已生成状态），点击【生成】可以重新生成管理密钥。如 0。

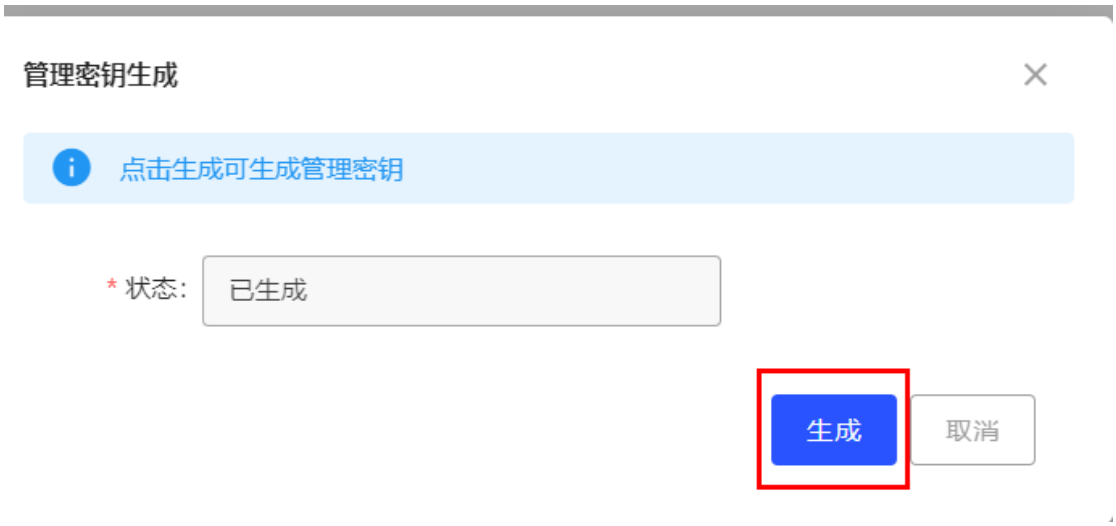

图3-119管理密钥生成

点击设备证书管理页面的【生成 P10】，在弹出框中选择密钥类型后，点击弹出框中的“生成 P10”按钮，如 0。如果密钥已经生成会提示“密钥已经生成，继续密钥将覆盖重新生成” 如 0。点击“确定”后弹出生成 P10 框，输入姓名、部门、单位、城市、省份点击【提交】，可生成设备 P10 请求文件，如 0。下载窗口如 0。

图3-120生成P10

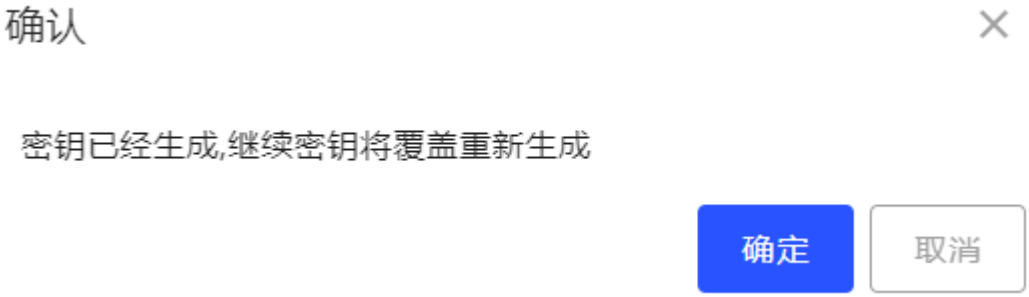

图3-121重复生成提示框

图3-122生成P10（2）

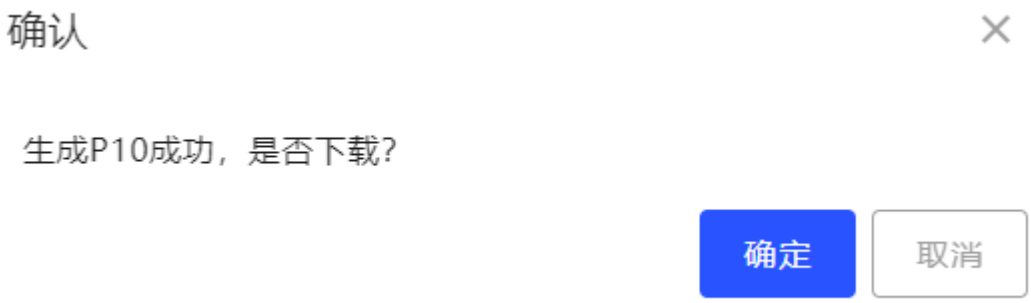

图3-123下载P10

点击【设备证书导入】选择要导入的设备证书如0，点击【导入】就可以导入设备证书，导入成功后证书会显示在下方设备证书列表中。界面如0。

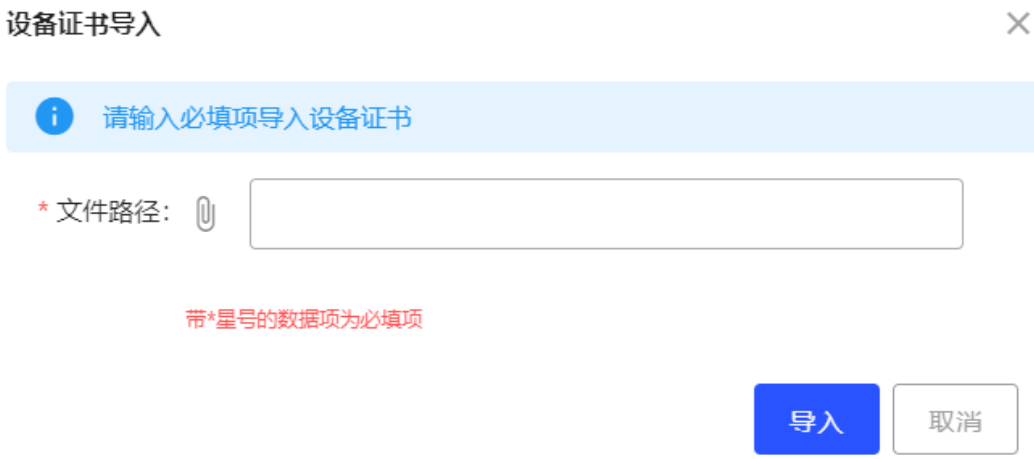

图3-124设备证书导入

图3-125设备证书列表

点击【设备加密密钥导入】选择加密密钥文件，输入密码，点击【导入】就可以导入设备加密密钥如0。

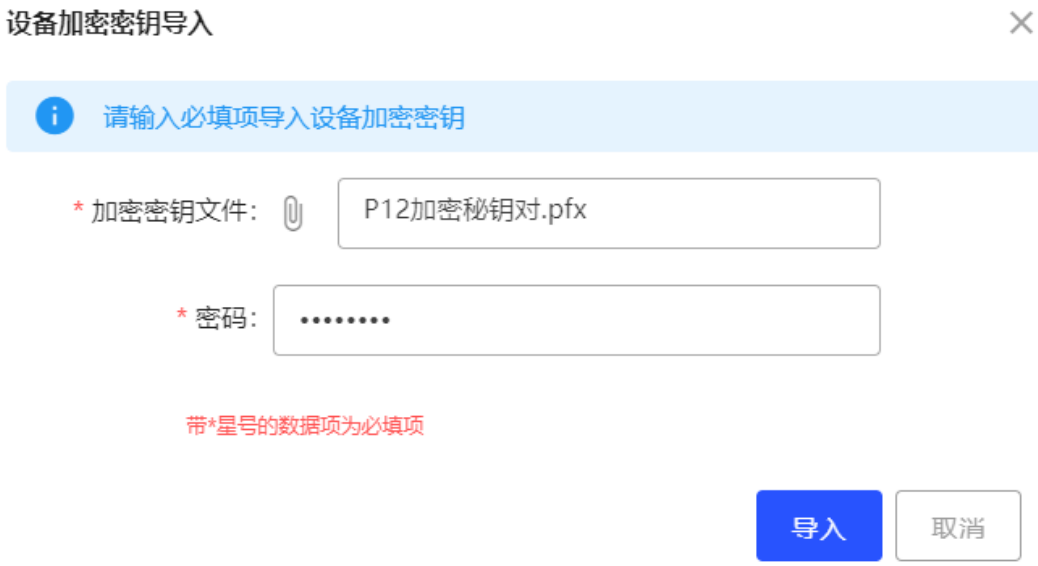

图3-126设备加密密钥导入

点击设备证书列表中的“删除” 如0，弹出提示框后，点击确定可删除对应的设备证书信息，如0。

图3-127删除设备证书

图3-128删除提示框

勾选证书所在行前的“□”，可多选，点击右上角【删除】按钮可以批量删除所选证书的信息如0。

图3-129设备证书多选删除

3.6.6 证书验证管理

证书验证管理包括验证证书有效期、验证证书签名有效性、验证证书是否在 CRL 中功能，点击“保存”，即可完成证书验证方式设置，界面如 0。

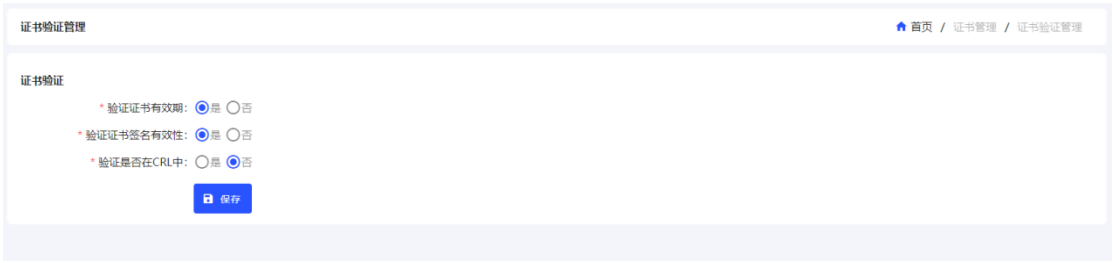

图3-130证书验证管理

3.6.7 证书同步设置

证书同步设置可以用于主服务向从服务进行证书同步，包括 CA 证书、CRL 证书以及用户证书，这些证书的新增以及更新操作都会同步到从服务。选择是否是主服务器，以及是否开启证书同步。主服务设置如图 3-131。**注：只有主服务器开启了证书同步，从服务才能进行连接。一台主服务器可以配置多台从服务器。证书的同步周期是 1 分钟。**

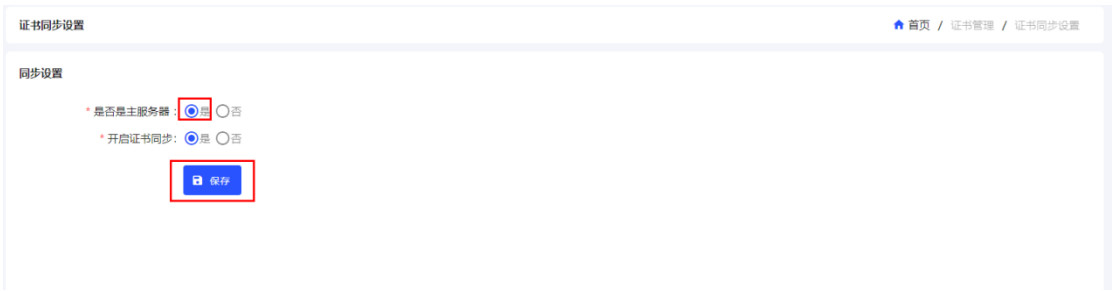

图3-131证书同步设置

是否是主服务器选择否且开启证书同步选择是从服务“是否是主服务器”选择否，即才可配置主服务 IP 和端口号信息,点击保存即可开启同步主服务器证书的功能如 0。关闭证书同步功能仅需将“开启证书同步”选择“否”，点击保存即可。

图3-132证书同步设置

3.6.8 数字信封管理

数字信封管理包括生成数字信封和数字信封解封(注：仅支持 SM2) 生成数字信封需要先创建 SM2 应用实体并导入加密证书。如 0。

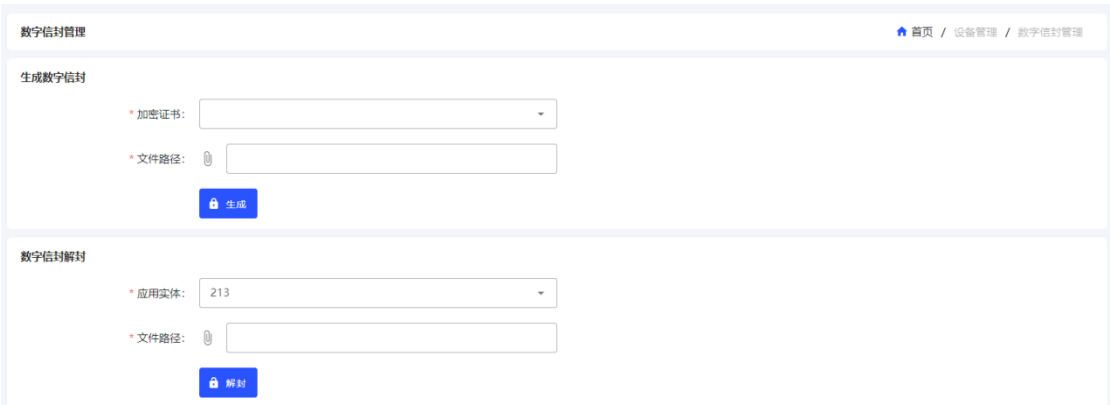

图3-133数字信封管理

选择加密证书和所需文件，点击【生成】就可以生成数字信封。如 0，数字信封文件生成成功，弹出是否下载弹出框，点击【确认】，下载数字信封文件，如 0。

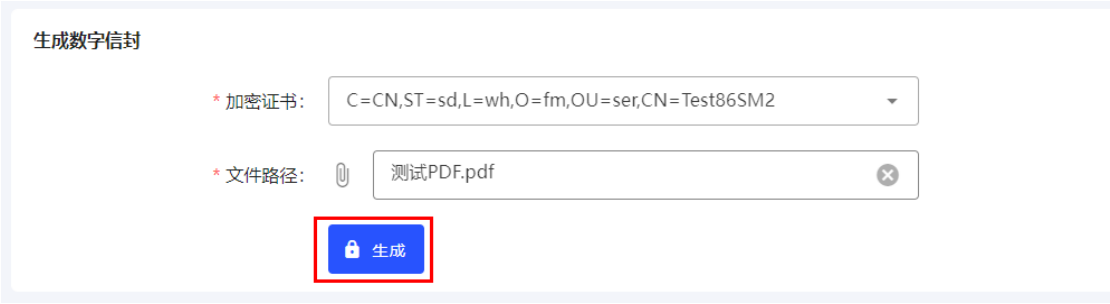

图3-134生成数字信封

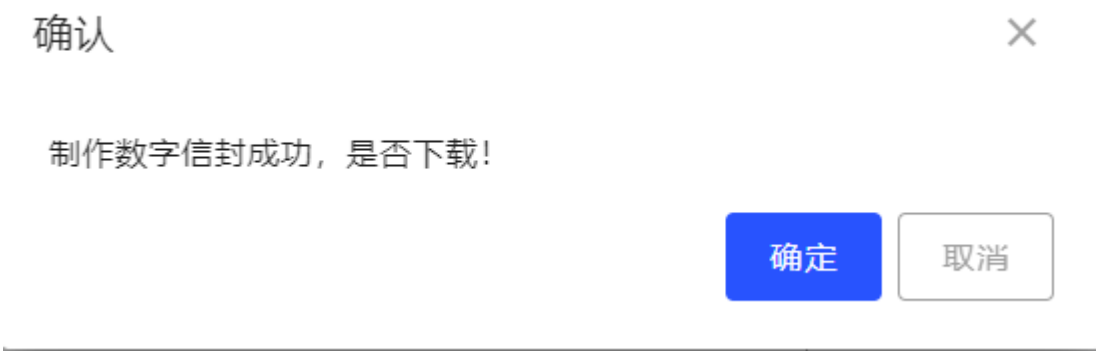

图3-135下载数字信封

选择应用实体和所需文件，点击【解封】就可以实现数字信封解封，如 0。数字信封解封后，会弹出是否下载原文数据的确认框，点击【确认】后，下载原文数据文件(文件后缀为.txt)，如 0。

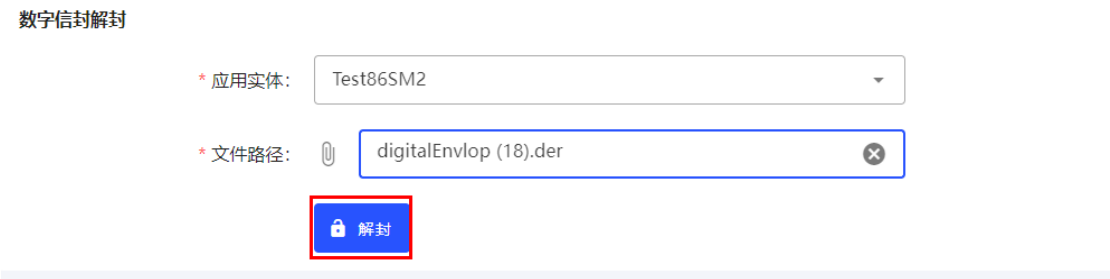

图3-136数字信封解封

图3-137下载原文件

3.7 日志管理

3.7.1 日志设置

日志设置包括日志等级的设置、Syslog 主机地址、清除日志、下载主服务日志功能。界面如 0。

图3-138日志设置

日志等级分为三个等级，分别错误日志 ERROR、调试日志 DEBUG、一般日志 INFO。

错误日志 ERROR：只记录页面操作错误或接口调用错误时的日志；

调试日志 DEBUG：记录重要功能调试信息的日志，同时包含错误日志 ERROR；

一般日志 INFO：记录详细处理过程信息日志，同时包含错误日志 ERROR 和调试日志 DEBUG。

界面如 0。选择日志等级，点击【保存设置】，可完成日志等级的修改。

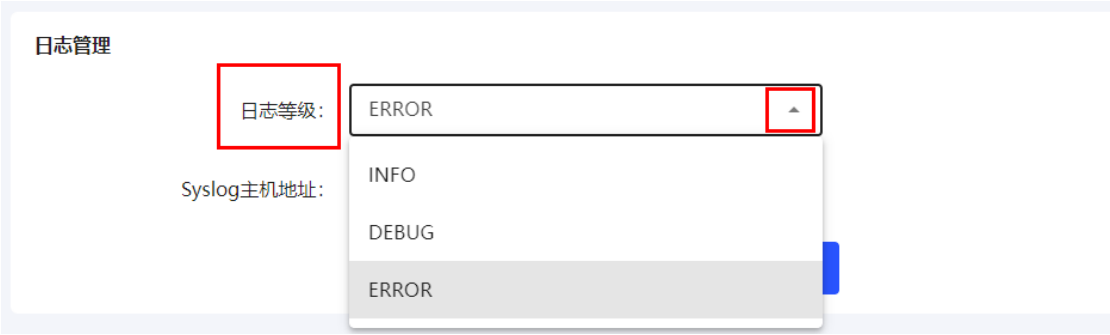

图3-139日志等级

若存在 Syslog 日志服务器,可在 Syslog 主机地址进行 IP 设置,点击【保存设置】,可完成配置。界面如 0。

图3-140Syslog主机地址

点击【清除日志】，可对系统存储的日志数据进行删除。界面如 0。

图3-141清除确认

点击【下载主服务日志】，可将系统主服务日志直接下载到本地。下载的文件如 0。

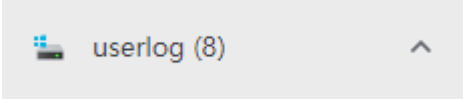

图3-142下载日志文件

3.7.2 日志审计（仅审计员可见）

日志审计列表显示查询到的日志信息，包括令牌序列号、操作信息、操作时间、HMAC和审计状态。界面如 0。

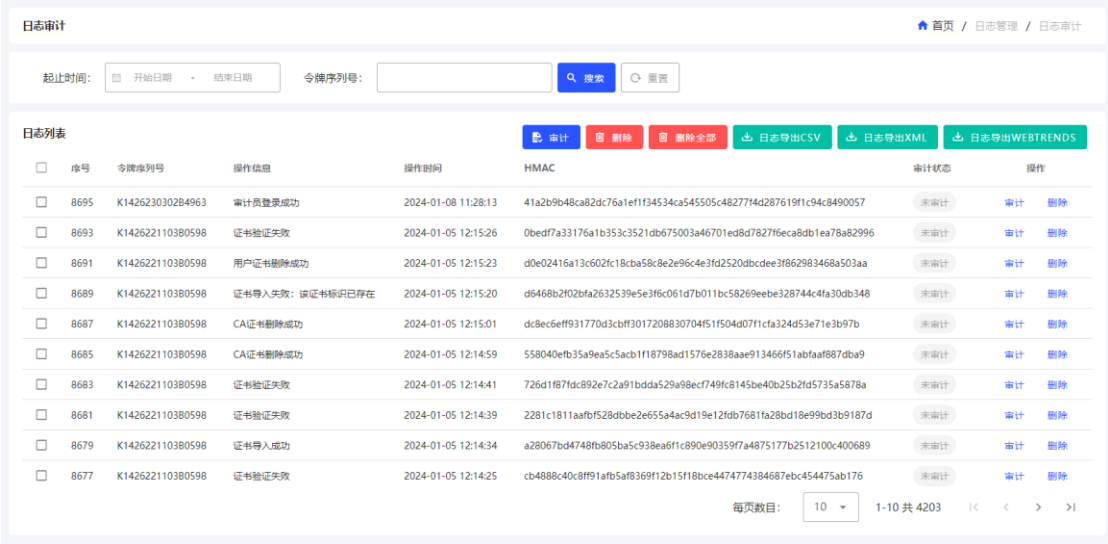

图3-143日志审计

可以通过输入令牌序列号或者日志时间，点击【搜索】按钮显示所对应的信息，点击【重置】按钮可以清除输入的查询条件。界面如 0。

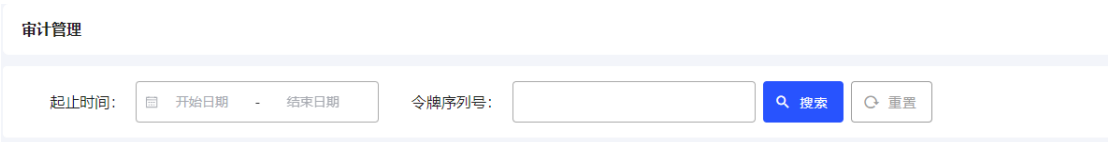

图3-144日志查询

选择需要审计的日志所在行，勾选序号所在行前“□”，可多选，点击【审计】，或点击列表对应记录所在操作列的“审计”按钮，如 0，日志审计完成之后，弹出日志审

计完成提示框(此处审计成功，为审计的操作成功，并不指审计结果)，如 0，日志审计成功之后，审计状态为：审计通过，如 0。若日志被篡改，则审计未通过，如 0，序号“37”原为“增加系统用户 K1426190507B4069 成功”，被篡改为“删除系统用户 K1426190507B4069 成功”，选择被篡改日志所在行，点击【审计】。审计完成之后，同样弹出日志审计完成提示框，如 0，日志审计失败之后，审计状态为：审计未通过，如 0。审计状态总共包括：未审计、审计通过、审计未通过（若日志被篡改，则审计未通过）。

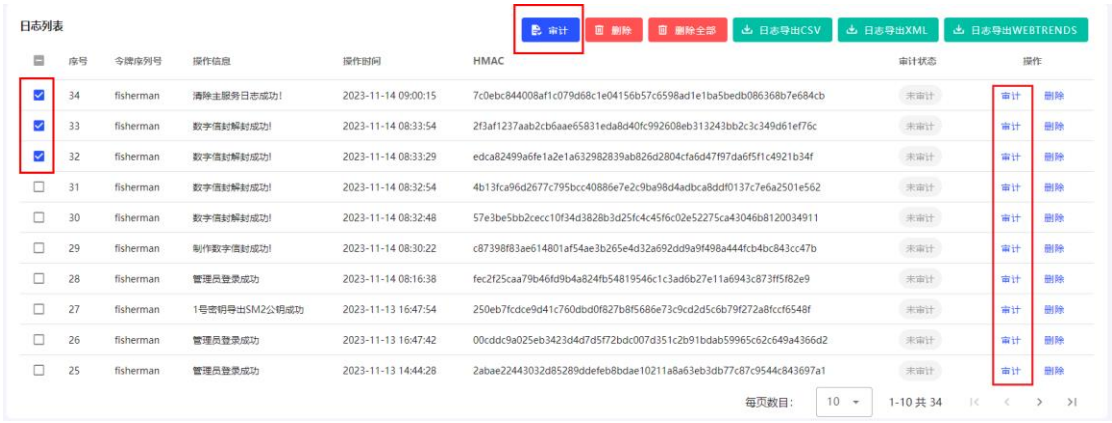

图3-145审计日志

图3-146审计成功

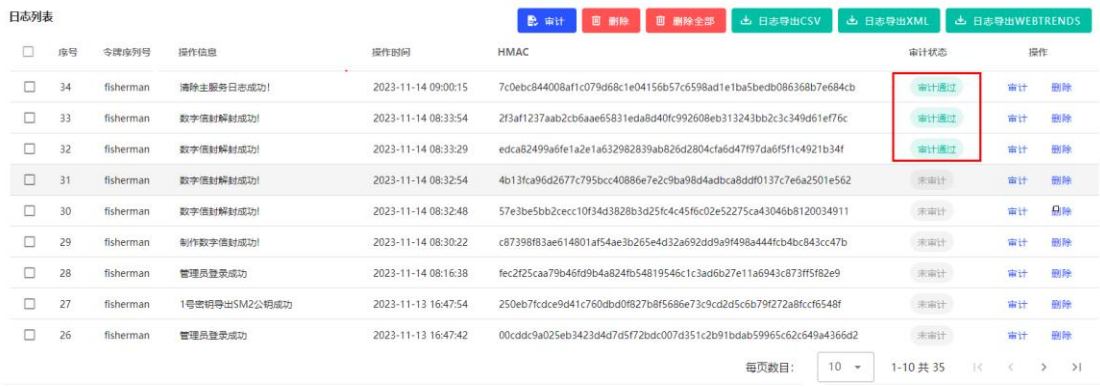

图3-147日志审计通过结果

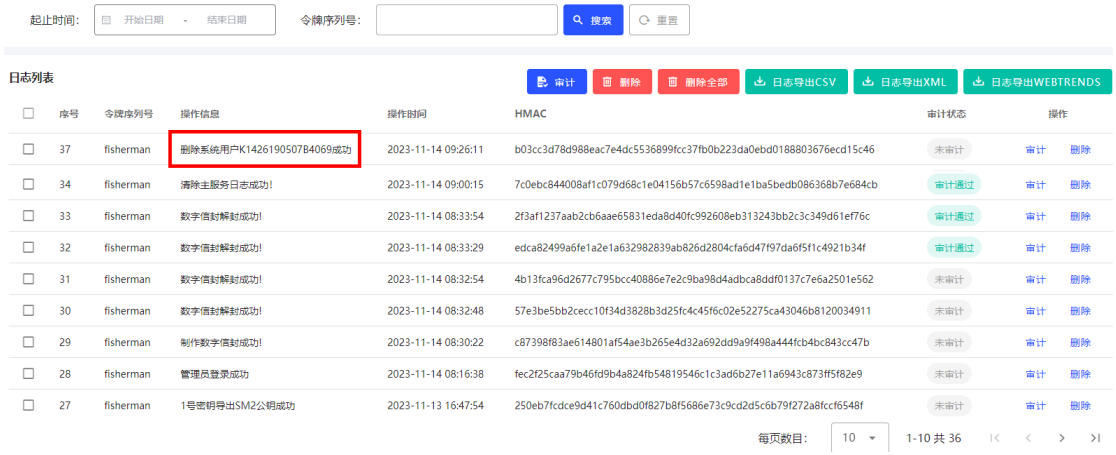

图3-148日志篡改

图3-149审计动作完成

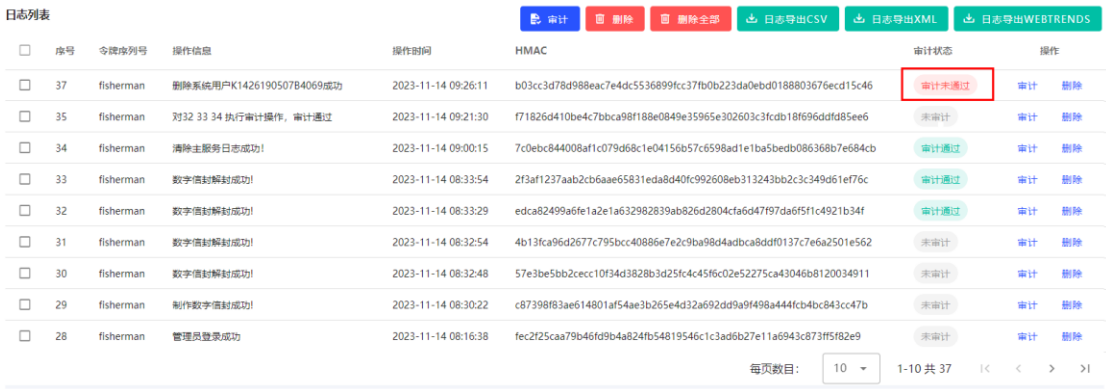

图3-150审计未通过

选择需要删除的一项或多项，勾选序号所在行前“□”，点击【删除】，或点击列表对应记录所在操作列的“删除”按钮，如 0，弹出确认提示框，如 0，确定后可以删除日志。

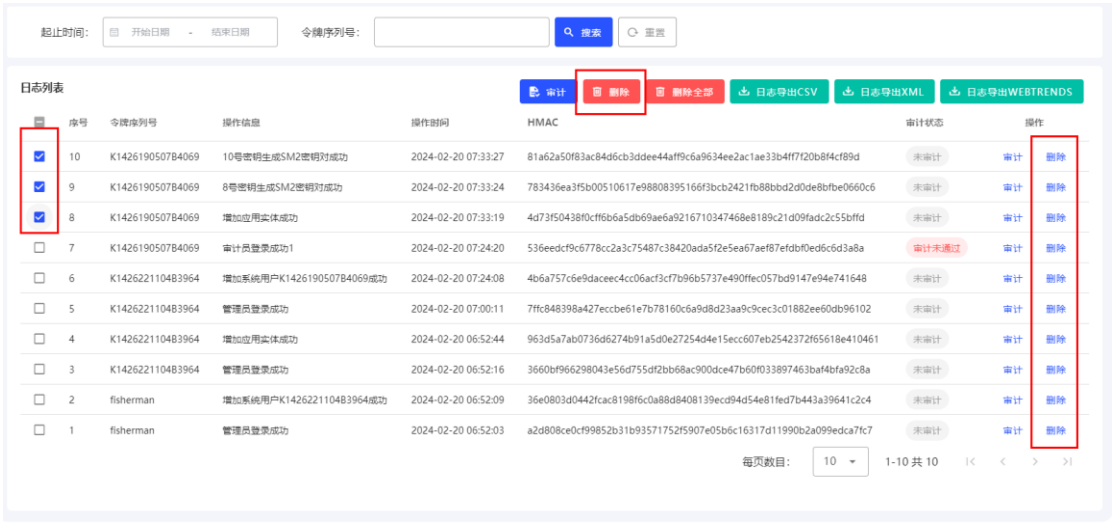

图3-151日志删除

图3-152删除提示

点击【删除全部】，如 0，弹出确认提示框如 0，点击确定后可以删除所有日志。

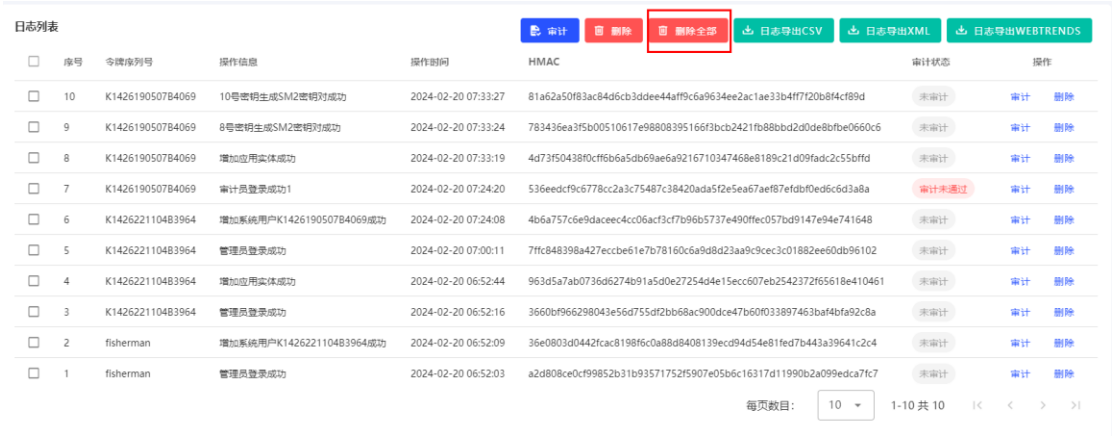

图3-153删除全部

图3-154删除全部提示框

分别选择开始时间和结束时间，可导出所选时间段的日志信息。如 0，然后点击【日志导出】（三种格式可选）可以导出对应时间的日志文件，如 0，时间不可为空。

图3-155日志导出

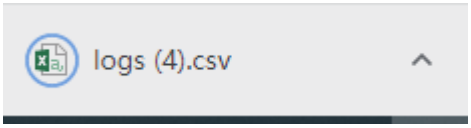

图3-156日志文件

3.7.3 故障日志

错误日志列表显示查询到的错误日志信息，包括操作时间、错误类型、设备 IP、设备端口号、错误码、错误描述、和排查方法。界面如 0。

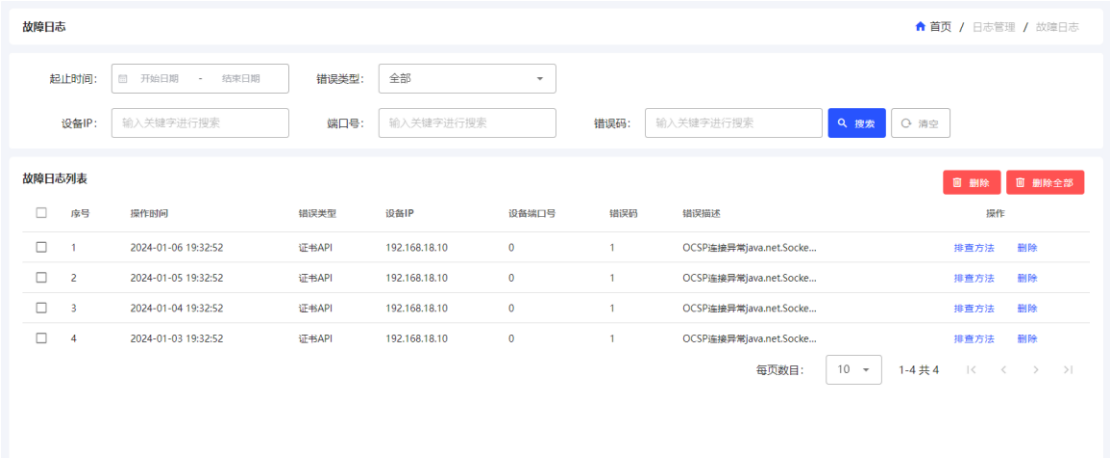

图3-157故障日志

可以通过选择起止时间、错误类型、设备 IP、端口号、错误码，点击【搜索】按钮显示所对应的信息，点击【清空】按钮可以清除输入的查询条件。界面如 0。

图3-158日志查询

选择需要删除的一项或多项，勾选序号所在行前“□”，点击【删除】按钮，或选点击对应记录“操作”列的“删除”按钮如 0，弹出确认提示框，如 0，确定后可以删除日志。

图3-159删除操作

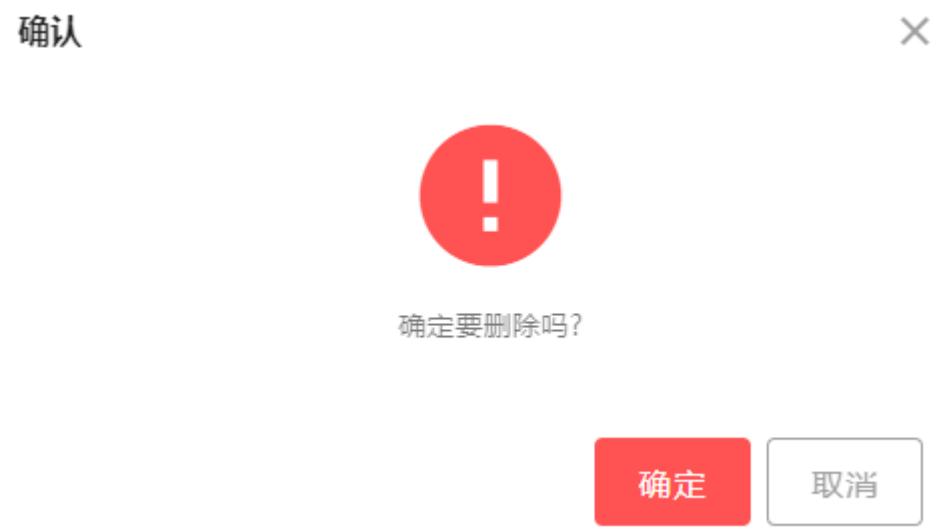

图3-160删除弹框

点击【删除全部】，如 0，弹出确认提示框，如 0，点击确定后可以删除所有日志。

图3-161删除全部

图3-162删除全部确认框

点击日志列表操作列的“排查方法” 如 0，弹窗可展示对应错误的解决方法信息，如 0。

图3-163排查方法

图3-164排查方法弹框（具体内容以实际显示为准）

3.8 预警管理

3.8.1 预警设置

预警阈值设置包括 CPU 占用率，内存占用率，磁盘占用率，并发连接数，网络负载，是否允许邮件告警等等，可以通过设置阈值来发出警告，界面如 0。

图3-165预警设置

“是否允许邮件告警”选择“是”，则显示邮件服务器相关配置，如 0。

图3-166邮件告警

3.8.2 预警列表

预警列表可以处理相关预警信息，包括预警信息的显示、查询、删除以及清除全部，界面如 0。

图3-167预警列表

选择起止时间，和预警类型，点击【搜索】按钮显示所对应的信息，点击【清空】按钮可以清除输入的查询条件。如 0。

图3-168搜索

勾选预警列表所在行前的“□”，可多选，点击【清除】可以删除所选预警信息，或通过点击操作列的“删除”，删除对应的预警信息。如图 3-169，点击【删除】会弹出是否删除的确认提示框，如 0。

图3-169预警信息删除

图3-170确认删除

点击【删除全部】，弹出确认提示框，如 0，点击确定后可以删除所有预警信息。

图3-171删除全部

3.9 国标密钥管理

3.9.1 SM2密钥

SM2 密钥显示当前密钥号下的签名/加密密钥对情况，包括签名/加密密钥对的生成、删除功能，界面如 0。

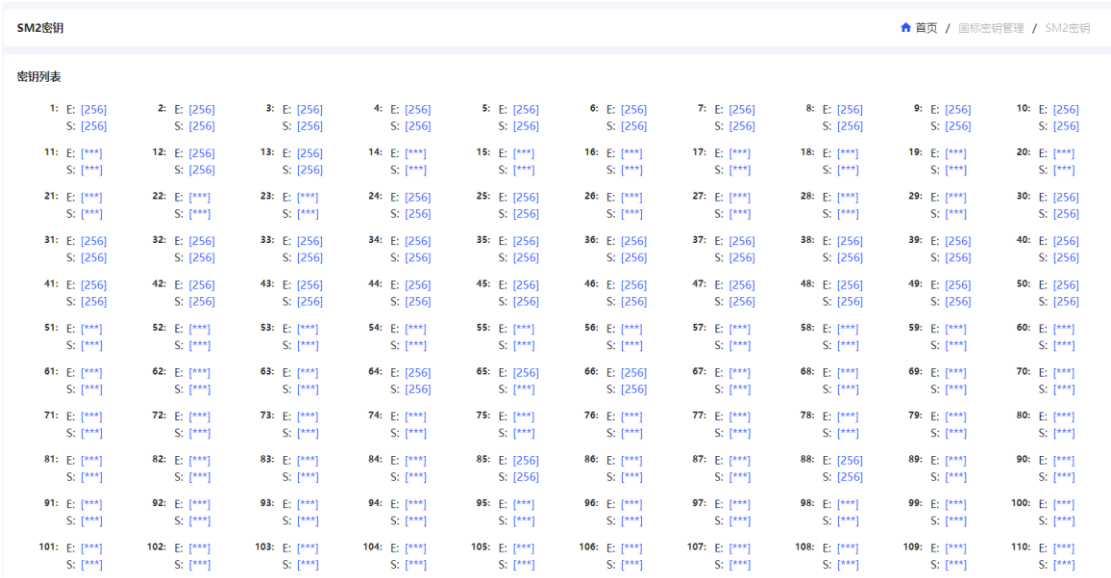

图3-172国标SM2密钥

选择密钥号，点击密钥号，界面如 0，默认显示密钥号以及类型，点击生成密钥，

可生成签名密钥对或加密密钥对；点击删除，可将该密钥号内的签名密钥对或加密密钥对进行删除。

图3-173国标SM2密钥生成/删除

点击【生成密钥】，则生成对应签名密钥对或加密密钥对，如果密钥已经存在，那么生成密钥会覆盖原密钥。界面如 0。

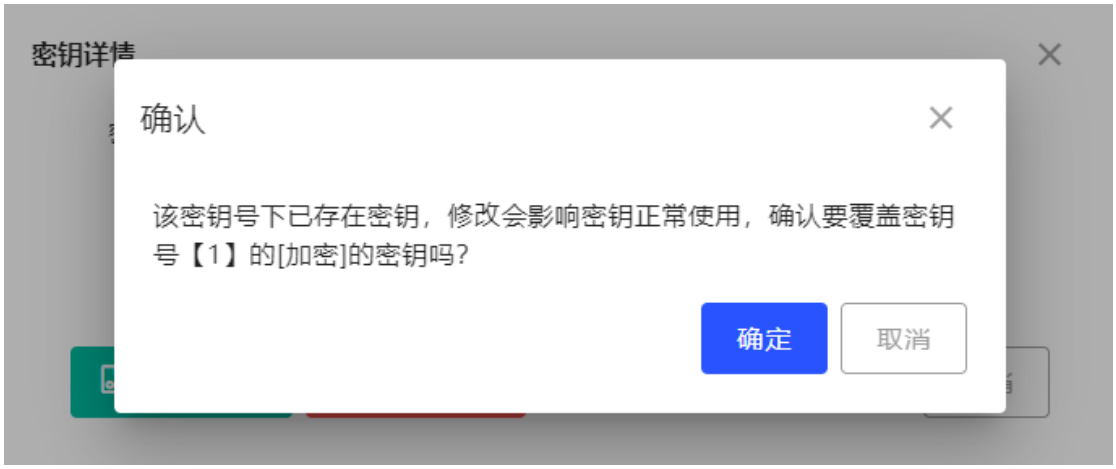

图3-174覆盖生成

点击【删除密钥】，可以将对应密钥对删除。界面如 0。如果密钥不存在则不能删除。界面如 0。

图3-175删除密钥

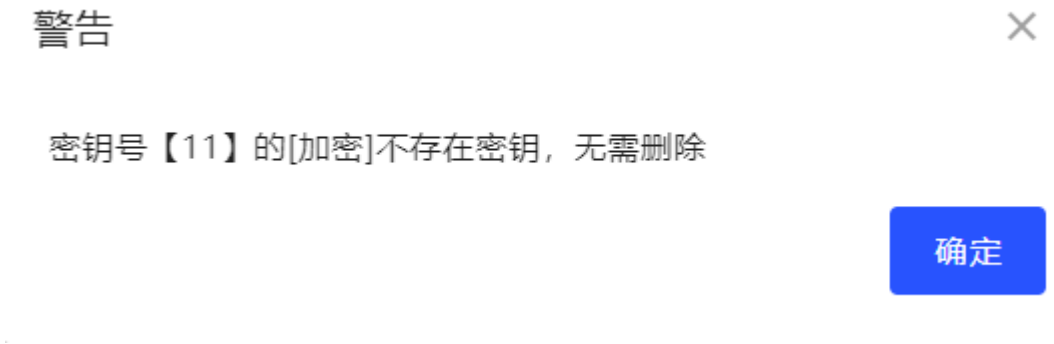

图3-176重复删除

3.9.2 RSA密钥

RSA 密钥显示当前密钥号下的签名/加密密钥对情况，包括签名/加密密钥对的生成、删除功能，界面如 0。

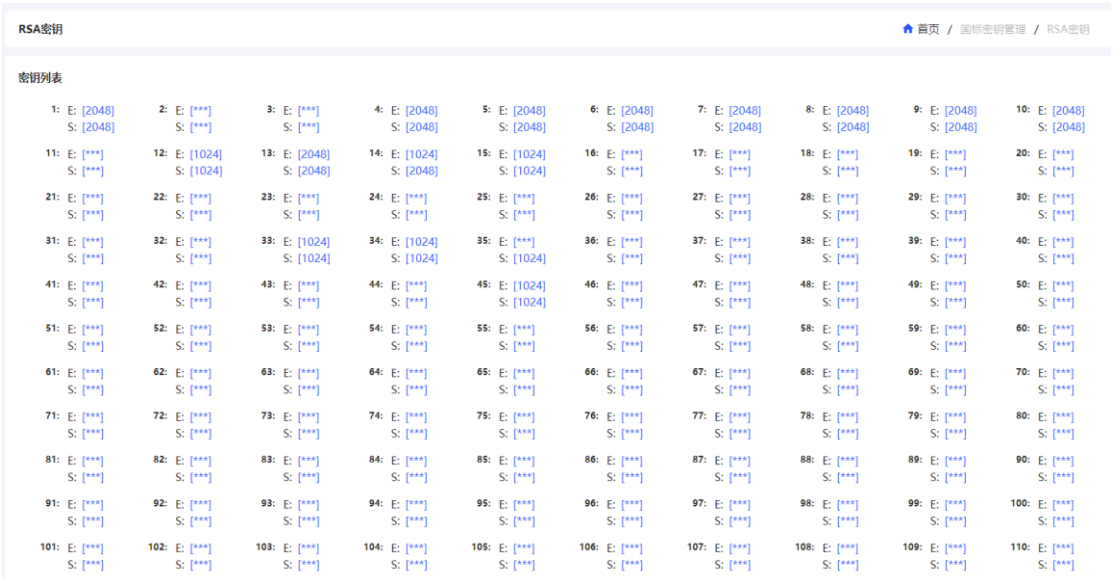

图3-177RSA密钥

在密钥列表点击要管理的密钥号，显示密钥信息，界面如 0。选择模长，点击“生成密钥”，可生成签名密钥对或加密密钥对；如果密钥已经存在，那么生成密钥会覆盖原密钥。界面如 0。

图3-178RSA密钥生成/删除

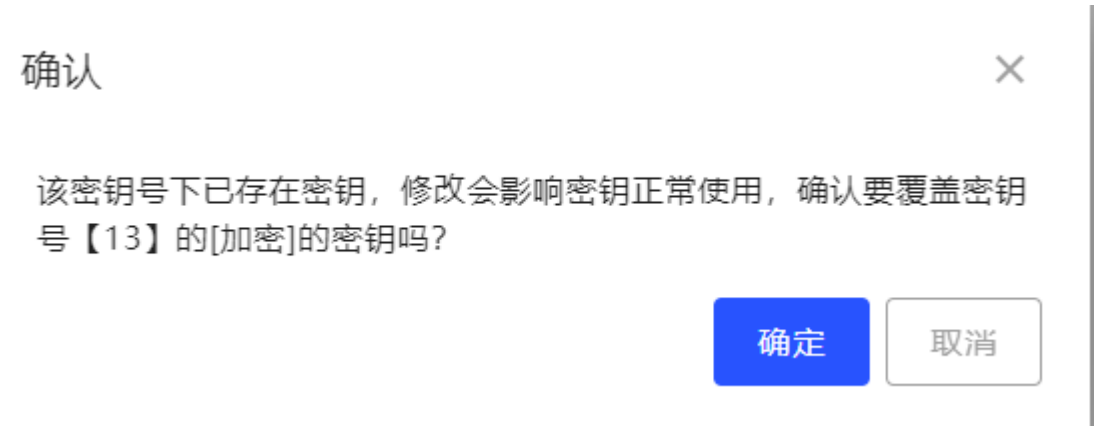

图3-179覆盖生成

点击【删除密钥】可以将对应密钥对删除。界面如 0。

图3-180删除密钥

如果密钥不存在则不能删除，模长 2048 同理。界面如 0。

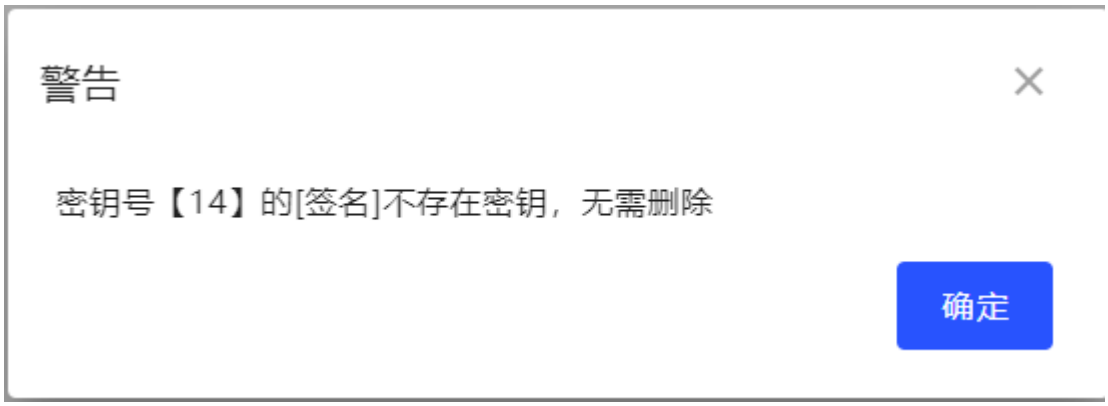

图3-181重复删除

3.9.3 对称密钥

对称密钥显示当前密钥号下密钥情况，界面如 0。

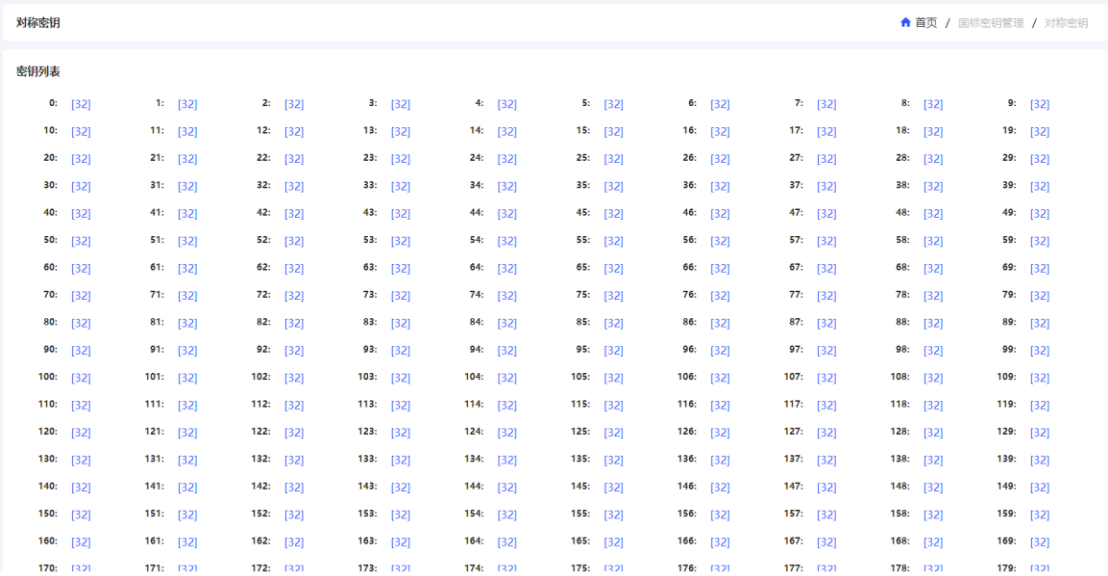

图3-182对称密钥

在密钥列表点击要管理的密钥号，显示密钥信息，界面如0。

图3-183对称密钥生成/删除

点击【生成密钥】，则生成对称密钥，如果密钥已经存在，那么生成密钥会覆盖原密钥。界面如0。

图3-184重复生成

点击【删除密钥】，则删除对称密钥。界面如0。如果密钥不存在则不能删除。界面如0。

图3-185删除密钥

图3-186重复删除

3.9.4 密钥批量管理

密钥批量管理，可以对可选范围内密钥进行批处理，包括RSA密钥、SM2密钥和对称密钥，主要功能为“批量生成”和“批量删除”，如0。

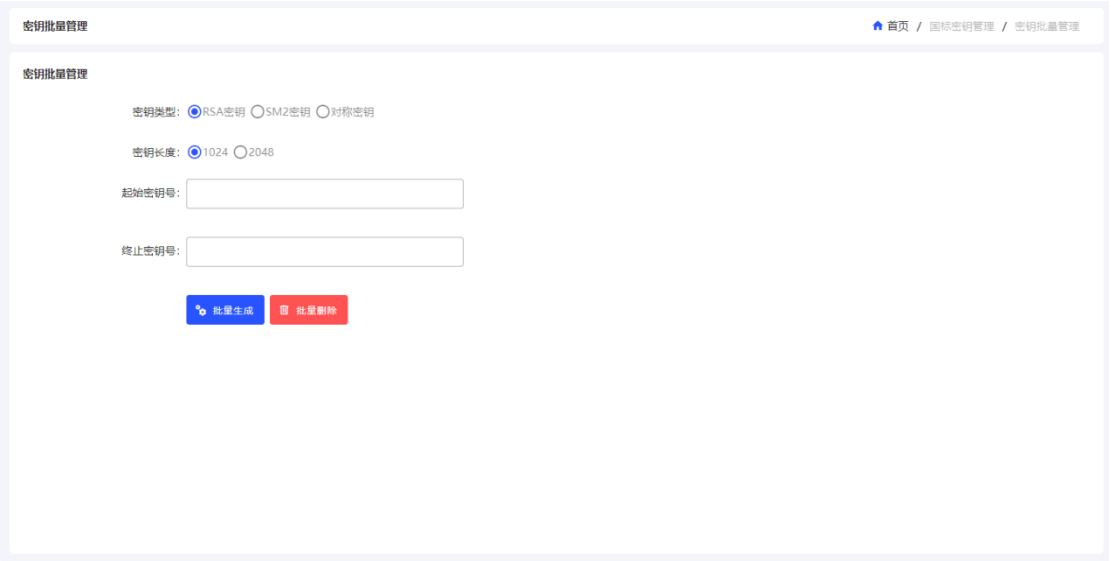

图3-187批量密钥管理

选择需要批量管理的密钥类型和密钥长度，RSA 密钥长度可选 1024 和 2048，SM2 密钥默认长度为 256 不显示，对称密钥长度也为默认长度 32 且不显示，输入正确的起始和终止密钥号，点击“批量生成”或“批量删除”，如果当前范围内存在密钥，则会弹出如 0 和 0 的确认弹出框，如果点击“确定”后生成或者删除操作将会覆盖该范围内所有已生成的密钥。

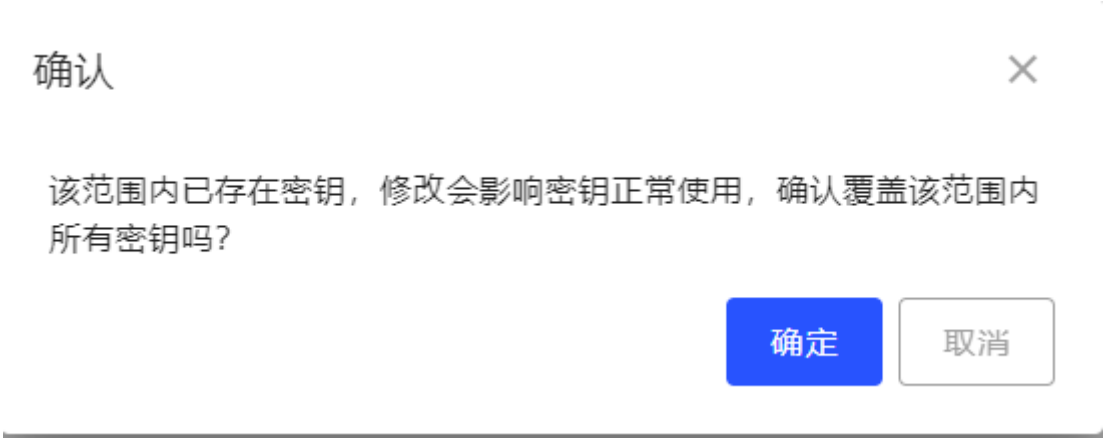

图3-188批量密钥生成/删除

图3-189批量密钥删除

当批量管理任务开始后会弹出如 0 的显示框，任务未结束前点击操作失效。

图3-190批量任务运行

当批量管理任务结束后弹出如 0 弹出框，表示批量管理任务已完成。

图3-191批量任务结束

当输入范围内不存在密钥时点击“批量删除”则会弹出如 0 的警告框。

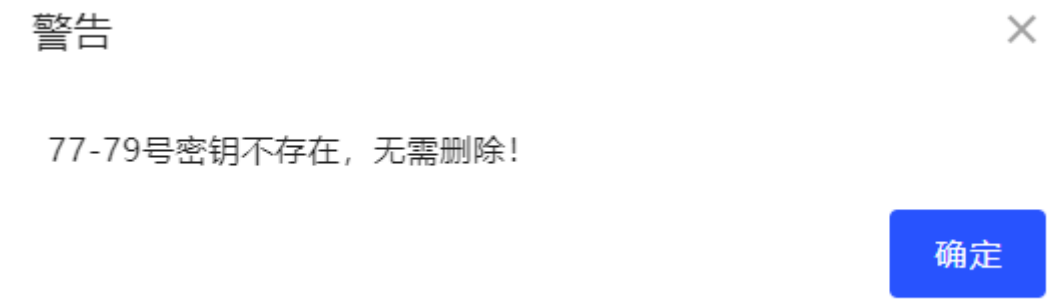

图3-192批量密钥删除

3.9.5 私钥权限码

私钥权限码管理显示当前密钥的私钥权限码信息(私钥权限码在创建应用实体时配置)。可以通过输入密钥号，点击【查询】按钮显示所密钥号的私钥权限码信息,【清空】可以清除输入的内容。界面如 0。

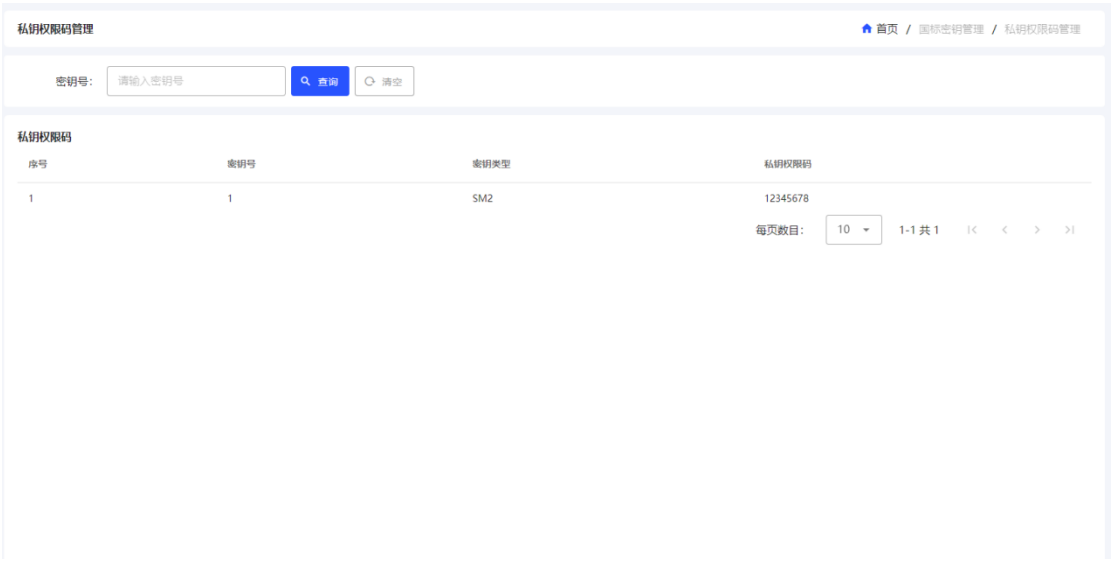

图3-193私钥权限码管理

4 初始化配置签名验签使用步骤

（本管理界面配置默认选择密钥类型SM2,若为RSA,步骤相同,只需注意选择密钥类型）

1、 打开初始化登录界面，下载 UKEY 组件安装，安装成功之后，使用默认用户名 fisherman 登录并新增管理员和审计员。（详见操作 3 产品操作说明）

2、 点击“证书管理”->“CA 证书管理”，导入 CA 证书（支持 cer 证书和证书链）。（详见操作 3.7.1 CA 证书管理）

3、 CA 证书导入成功之后，点击“证书管理”->“证书验证设置”，进行证书验证设置。默认设置为验证证书有效性和验证证书签名有效性。说明：若设置验证是否在 CRL 中，需要点击“CRL 管理”导入 CRL 或点击“证书管理”->“证书状态查询设置”设置 CRL 自动更新。（详见操作 3.7.2 证书验证设置/3.7.4CRL 管理/3.7.5 证书状态查询设置）

4、 点击“应用实体管理”->“应用实体注册”，注册应用实体。

5、 应用实体注册成功之后，点击“应用实体管理”->“应用实体信息管理”，选择应用实体所在行，点击“生成 P10 请求”，输入 P10 信息，点击“签名证书 P10

生成”和“加密证书 P10 生成”。成功之后下载签名 P10 和加密 P10 ，通过证书注册系统生成签名证书和加密证书，点击“导入证书”，导入签名和加密证书（详见操作 3.2 应用实体管理）

以上步骤成功操作完成之后，可正常使用签名验签服务器，若需其他功能，可根据用户手册进行其他功能配置。

5 常见问题及解答

1、问：用户登录用户时，已经插入 Ukey，输入密码，点击登录却提示“令牌打开失败，请确认是否插入令牌!”。

答：因为由于登录时插入的 Ukey 部件版本可能比较低，不能立即识别。此时可点击下拉列表，刷新 Ukey 的序列号，再点击登录即可。

2、问：私钥权限码管理中为什么只有私钥权限码的查看功能？

答：因为在应用实体注册的过程中，会有设置私钥权限码的步骤，应用实体注册过程中密钥号对应的私钥权限码同步设置，应用实体删除过程中，对应密钥号的私钥权限码也会同步删除。

3、问：时间配置中设置系统时间后，点击其他功能无反应？

答：因为系统设置 session 有效期为 30 分钟，如果设置的时间与当前时间相差 30 分钟以上，当前 session 有效期将失效，系统会自动退出当前用户登陆状态，此时需重新执行登录系统操作。

4、问：设备提供数字签名、验签服务的准备工作有哪些？

答：设备已执行完成初始化；配置网络地址、设备时间；添加 5 个管理员、1 个审计员；在证书管理功能模块中导入 CA 证书；在应用实体管理模块中注册应用实体，生成应用实体的签名密钥对和加密密钥对,设置私钥权限码(注意:此码用于调取密钥，不可丢失、遗忘，可在其它地方进行安全备份)，导入应用实体的数字证书；应用实体依据 GM/T 0018-2012《密码设备应用接口规范》、GM/T 0029-2014《签名验签服务

器技术规范》标准进行 API 接口配置。

5、双机热备开启之后，点击数据同步，提示“数据同步失败”，但是实际数据同步成功？

答：在建立数据同步通道的过程中，有时会存在时间延迟，当查询数据同步是否建立时，若数据同步通道正在建立中，则会提示数据同步失败，过几分钟重新刷新页面再次点击数据同步，若数据同步已经成功，则会给予成功提示，若仍然失败，则给予失败提示。

6、数据同步开启正常运行中，登录子服务 IP 操作，无法正常同步数据？

答：数据同步开启后，需访问主服务 IP，请勿再访问子服务 IP 操作。因数据同步开启后，会存在主备切换，本设备数据同步原理为“主同步从，从不能同步主”，若数据同步开启正常运作之后，仍然访问子服务 IP 操作，若恰巧访问的是从设备，从设备记录日志等其他数据表 ID 会与主设备 ID 产生冲突，而导致数据同步失败。