安为科技

AnweiTech

视频安全服务系统

操作手册

法律声明

版权所有©北京安为科技有限公司 2021。保留一切权利。

本手册从的任何部分，包括文字、图片、图形等均归属于北京安为科技有限公司（以下简称“北京安为”或“安为科技”）。未经书面许可，任何单位或个人不得以任何方式摘录、复制、翻译、修改本手册的全部或部分。除非另有约定，北京安为科技有限公司不对本手册提供任何明示或默示的声明或保证。

关于本手册

本手册仅作为相关产品的指导说明，可能与实际产品存在差异，请以实物为准。因产品版本升级或其他需要，北京安为科技有限公司可能对本手册进行更新，如您需要最新版手册，请您登录公司官网查阅。（http://www.anweitech.com）。

建议您在专业人员的指导下使用本手册。

商标声明

安为科技 AnweiTech 为安为科技的注册商标。本手册涉及的其他商标由其所有人各自拥有。

责任声明

●在法律允许的最大范围内，本手册以及所描述的产品（包含其硬件、软件、固件等）均“按照现状”提供，可能存在瑕疵或错误。北京安为不提供任何形式的明示或默示保证，包括但不限于适销性、质量满意度、适合特定目的等保证；亦不对使用本手册或使用本产品导致的任何特殊、附带、偶然或间接的损害进行赔偿，包括但不限于商业利润损失、系统故障、数据或文档丢失产生的损失。

●您知悉互联网的开放性特点，您将产品接入互联网可能存在网络攻击、黑客攻击、病毒感染等风险，北京安为不对因此造成的产品工作异常、信息泄露等问题承担责任，但北京安为将及时为您提供产品相关技术支持。

●使用本产品时，请您严格遵循适用的法律法规，避免侵犯第三方权利，包括但不限于公开权、知识产权、数据权利或其他隐私权。您亦不得将本产品用于大规模杀伤性武器、生化武器、核爆炸或任何不安全的核能利用或侵犯人权的用途。

●如本手册内容与适用的法律相冲突，则以法律规定为准。

前言

本部分内容的目的是确保用户通过本手册能够正确使用产品，以避免操作中的危险或财产损失。在使用此产品之前，请认真阅读产品手册并妥善保存以备日后参考。

符号说明

符号	说明
	说明类文字，表示对正文的补充和解释。
	注意类文字，表示提醒用户一些重要操作或者防范潜在的伤害和财产损失危险。
	警告类文字，表示有潜在风险，不过不加避免，有可能造成伤害事故、设备损坏或业务中断。

安全注意事项

- 视频安全一体机的安装施工须符合规范，可参照相关国家标准或地方标准。
- 若将视频安全一体机安装在高空或其他不安全环境下时，请务必保证安装过程中的安全措施，以免发生意外。
- 视频安全一体机应工作在技术指标允许的温度及湿度范围内。
- 安装本产品应由专业的服务人员进行，并将视频安全一体机安装在儿童、老人及其他特殊人群所不能触碰的空间，以免发生不安全事件。

- 若视频安全一体机在非正常工作的情况下出现如冒烟、有异味等极其异常的情况时，请立即断开电源线，停止使用本机，并与经销商或客服联系，不要以任何方式拆卸或修改产品。（未经认可的修改或维修导致的问题，本公司不承担任何责任）。
- 请定期对视频安全一体机进行保养与维护，以便能延长其安全使用年限。

- 设备接入互联网可能面临网络问题，请您加强个人信息及数据安全保护。当您发现设备存在安全隐患时，请及时与我们联系。
- 请妥善保存视频安全一体机的全部原包装材料，以便出现问题时，使用包装材料将产品包装好，返回厂家处理。非原包装材料导致的运输途中的意外损害，由使用者承担责任。

1. 产品简介

1.1 产品说明

AWS-SecMFS 系列视频信息安全一体机，主要用于对已建视频监控平台根据 GB 35114-2017 标准要求进行安全性加固。该产品采用国家商用密码算法模块和高性能处理器，可为已装安防视频监控设平台提供符合 GB 35114-2017 C 级标准设备身份认证，以及基于 H.264/265/SVAC2.0 码流格式的视频流加密解密、视频关键帧签名验签等安全功能。

该产品可广泛用于军队、保密、公安以及其他对视频安全防护要求较高的行业和场所，可以对无安全防护措施的视频平台提供便利的安全加固，快速实现基于商用密码算法的平台安全性提升。

1.2 产品功能

身份信息认证

- 平台内元素统一编码
- 数字证书与平台元素对应，避免非法元素具有合法身份
- 基于证书实现平台元素的身份认证，避免非法元素接入
- 分级管理，减少性能损失

SIP 信令完整性校验

- 对设备遥控等重要 SIP 信令做消息认证，避免被篡改
- 利用商用密码中的杂凑算法实现对控制信令消息的防护
- 支持跨域控制指令的鉴权和认证

视频流数据签名

- 支持视频数据关键帧签名，避免重要数据被篡改
- 支持签名视频数据的接收、存储和验证，确保视频完整性和视频源抗抵赖

视频流数据加密

- 对重要点位设备的视频进行加密传输，避免重要视频资料被窃取

- 支持加密视/音频信息的播放、回放、存储和分发
- 支持密钥生成、更新和管理

1.3 产品参数

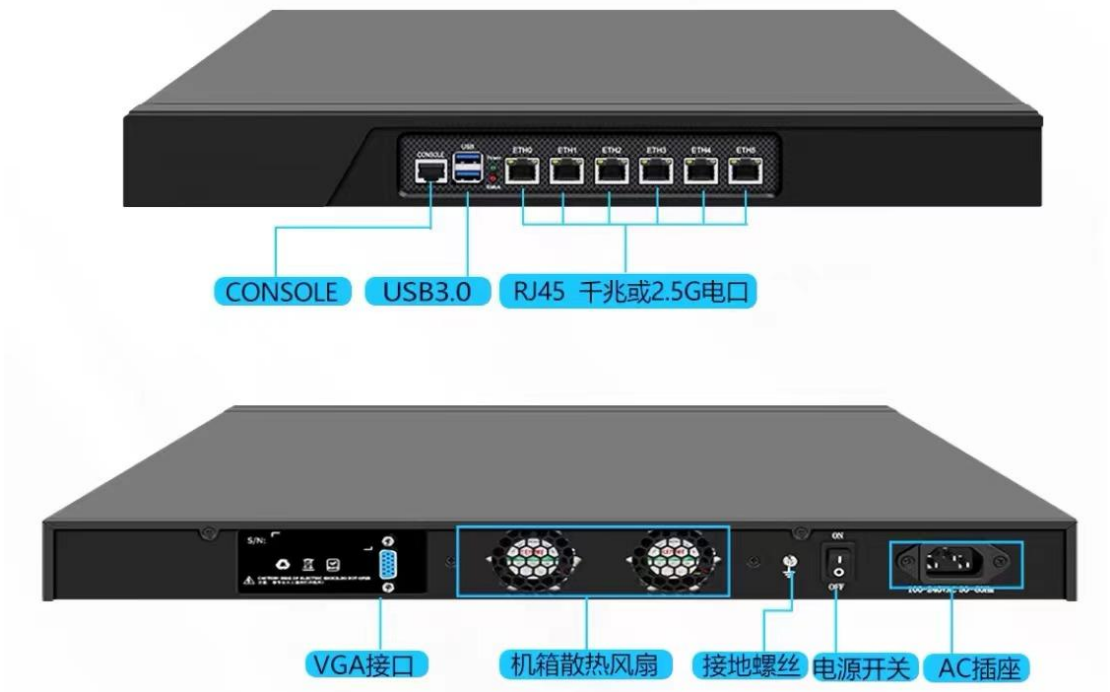
规格/型号		AWS-SecMFS-MN
一般规范	产品尺寸	440mm*250mm*44mm
	工作温度	-20℃~+60℃
	工作湿度	5%~95% RH 不凝结
	电源电压	100-240V~50/60HZ
视频	视频压缩标准	H.264、H.265、SVAC
	H.264 编码类型	Main Profile/High Profile
	H.265 编码类型	Main Profile
	SVAC 编码类型	SVAC2.0
	支持视频路数	100 路
	视频流协议	RTP、RTSP
网络	网络接口	6*RJ45 接口 10/100M/1000M 自适应以太网
	网络协议	HTTP,TCP/IP,ICMP.RTSP,RTP,UDP,RTCP,SMTP,DHCP,DNS
	接入协议	GB 35114-2017、GB/T 28181、ONVIF、RTSP
	输出协议	GB 35114-2017、GB/T 28181、RTSP
	通用功能	心跳、密码保护
安全	密码算法	SM1、SM2、SM3、SM4、RSA、AES
	视频安全功能	支持 H.264/H.265/SVAC 视频流的加密、解密、签名、验签
	网络安全功能	支持协议、端口、IP 白名单配置
管理	设备配置	支持设备的 Web 界面安全登录，可对 SIP 信令、IP 地址、端口等进行配置。可在线升级软件版本，支持对升级文件进行签名校验和更新成功与否反馈的功能。支持 NTP、手动两种模式的时间校时，支持平台的用户管理，支持用户采用 UKey 等方式进行安全登录。
	设备管理	支持展示前端视频安全转换器的状态信息，包括基础信息、设备状态信息、告警信息、流量统计信息等。支持视频安全服务在线升级视频安全加固终端软件版本，支持对升级文件进行签名校验和更新成功与否反馈的功能;支持对视频安全转换器终端设备的管理，支持设备导入、批量配置管理、批量更新、批量证书同步、批量证书签发等功能。
	视频功能	支持视频安全服务及运维管理平台对前端视频的预览，对视频进行加密、解密、签名和验签操作，支持对相机云台的安全控制等。

1.4 产品外观

视频信息安全一体机为标准 1U 机架式服务器，主机尺寸 440×252*45mm,

设备外观与接口如下图 1-1 所示：

图 1-1 产品外观图



标识	说明
CONSOLE	管理和配置的物理接口。
USB	USB 接口。用于连接 U 盘、鼠标等设备。
LAN	LAN 以太网口。

WAN1~WAN5	以太网口。RJ45 千兆或 2.5G 电口。
VGA	VGA 接口。用于连接显示器的 VGA 接口。
⏚	接地端。
ON～OFF	电源开关键。
100~240VAC 50/60Hz	电源输入。

2. 操作须知

2.1 系统登录与退出

登录系统

说明

当安装好前端视频设备、视频安全转换器和视频安全一体机后，您可在浏览器中输入视频安全一体机的 IP 地址 https://192.168.0.2 登录。首次登录视频安全服务系统默认登录管理员账号，用户名：admin，密码：123456，点击“登录”按钮，进入系统。如图 2-1 所示。

“admin”为系统管理员用户，为了系统安全性，建议您使用新增的用户进行操作，添加用户具体步骤请参见用户管理。

用户连续输入 6 次错误密码，系统提示账号锁定，管理员通过“忘记密码”界面找回密码，普通用户需联系管理员重置密码。

图 2-1 视频安全服务系统登录

退出系统

当进入视频安全服务系统主界面时，您可点击右上角的" 注销 "，安全退出系统。

2.2 主界面说明

在视频安全服务系统里面，您可以进行系统配置、视频预览功能，界面如图 2-2 所示。

图 2-2 主界面

说明

配置：对视频安全一体机进行系统配置及功能配置。

预览：用于网络摄像机监控画面预览、视频加解密、签名、验签操作及参数调节。

3. 系统参数设置

系统模块包括系统设置、系统维护、用户管理三个子模块，界面如图 3-1 所示。

3.1 系统状态

选择“配置→系统→系统设置”，单击“系统状态”页面，可查看视频安全一体机的 CPU、网络、磁盘、内存运行情况。如图 3-1 所示。

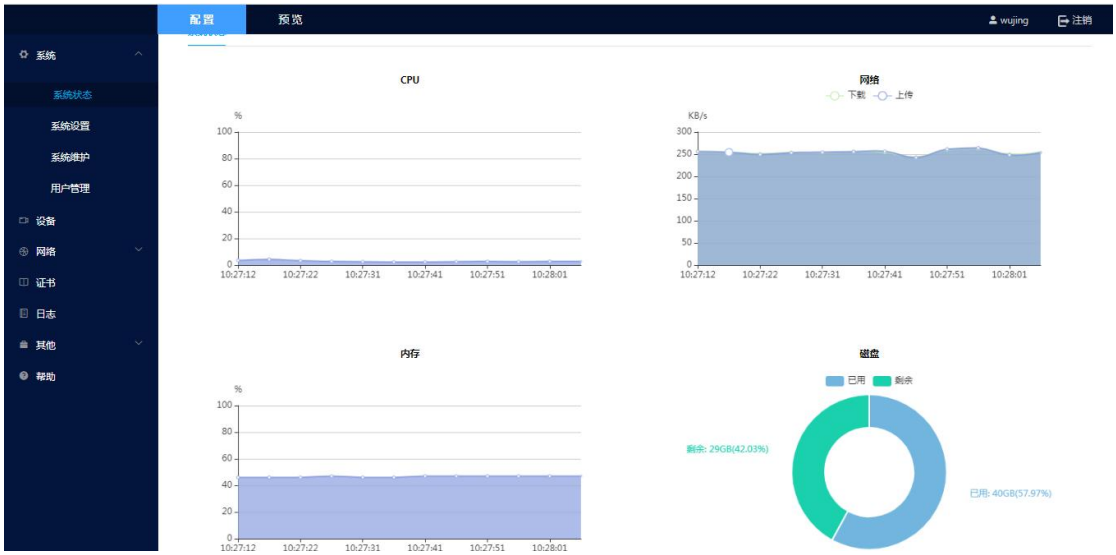


图 3-1 系统状态

3.2 系统设置

系统设置包括系统状态、基本信息、时间配置和 NTP 服务。

3.2.1 基本信息

选择“配置→系统→系统设置”，单击“基本信息”页面，可查看视频安全一体机的基本信息。

基本信息提供的内容包括设备类型、设备序列号、主控版本、Web 版本、通道总数和磁盘总数的信息，上述信息均从设备中读取，无法手动修改。如图 3-2 所示。

图 3-2 基本信息

3.2.2 时间配置

选择“配置→系统→系统设置”，单击“时间配置”页面可对视频安全一体机时区进行校时，界面如图 3-3 所示。

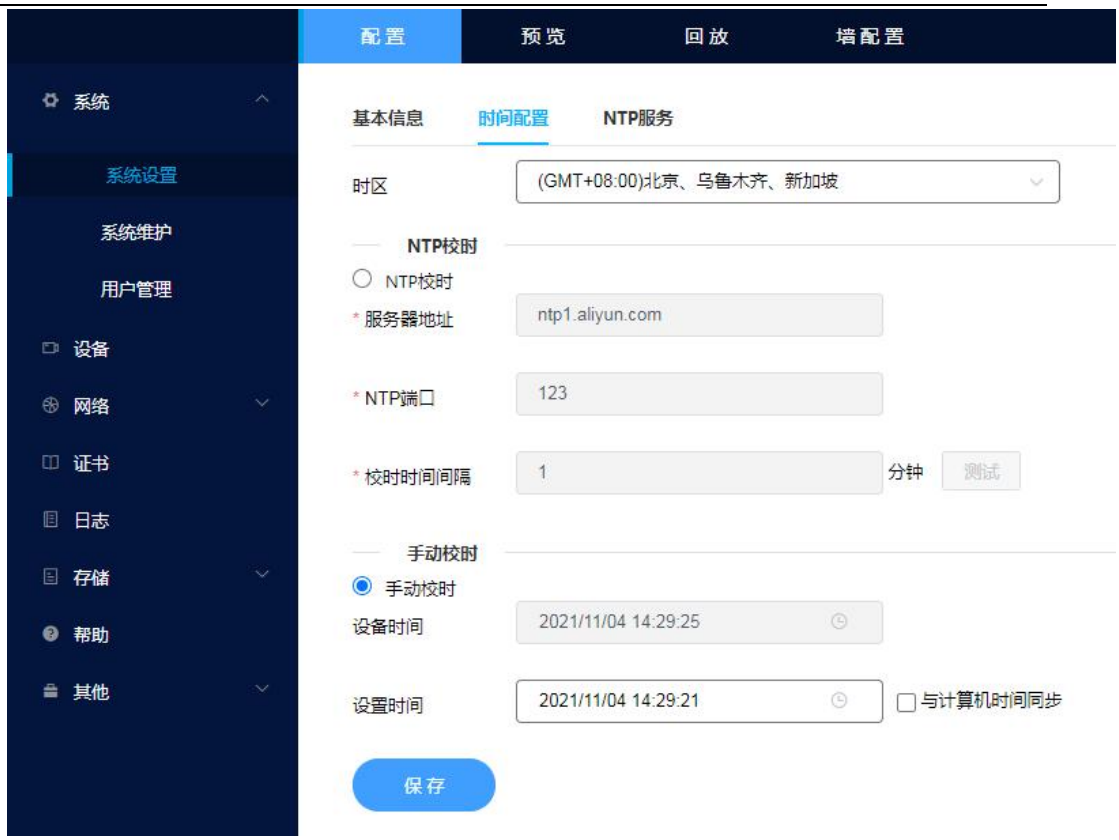


图 3-3 时间配置

说明

设备时区：进入时间配置界面，可以对视频安全一体机进行校时。“时区”选择当前设备所在的时区并可根据实际情况进行设置。系统默认选择“(GMT+08:00)北京、乌鲁木齐、新加坡”。

时间校时有两种方法，NTP 校时（即网络校时协议）和手动校时。

（1）NTP 校时

您可设置 NTP 服务器地址、NTP 端口号和校时时间间隔，设备即按照设置每隔一段时间校时一次，设置完成后可以单击“测试”检测视频安全一体机与 NTP 服务器之间连接是否正常。

（2）手动校时

勾选“手动校时”，手动校时有两种方式，一、单击设置时间框，需要手动选择日期和时间。二、选中与计算机时间同步的选择框“ ”，选择之后，设置时间与计算机上的时间同步。

时间设置完成后，单击“保存”完成参数配置。

3.2.3 NTP 服务

NTP 服务的端口号和协议信息，界面如图 3-4 所示。

图 3-4 NTP 服务

3.3 系统维护

选择“配置→系统→系统维护”，单击“系统维护”进入系统维护界面。界面如图 3-5 所示。

图 3-5 系统维护

说明

（1）系统重启，单击“重启”，重启系统。

（2）系统恢复

系统恢复分为简单恢复和完全恢复。

简单恢复是将除 IP 地址、子网掩码、网关、用户信息和制式等信息以外的

其他系统参数恢复到出厂设置。

完全恢复是将所有系统参数恢复到出厂设置。

（3）系统升级

当系统需要升级时，用户需要将升级的文件拷贝到本地计算机当中，进入“系统→系统维护”，单击“选取文件”选择本地升级文件，单击“升级”。如文件错误，提示“升级失败”，如文件正确，提示“设备将会重启，请确认是否升级”，单击确定，升级完毕后系统自动重启系统。系统完成升级后跳转至登录页面。

3.4 用户管理

选择“配置→系统→用户管理”进入用户管理界面，可以对视频安全服务系统操作用户进行设置，当前用户为管理员“admin”时，用户可根据需要创建其他用户，最多可以创建 10 个用户，界面如图 3-6 所示。

图 3-6 用户管理

3.4.1 用户添加

选择“配置→系统→用户管理”，进入用户管理界面，单击“添加”，弹出用户添加界面，输入用户名、选择用户类型、输入密码、密码确认、选择用户权限。如图 3-7 所示。

图 3-7 用户添加

注意

- 为了更好的保护用户隐私并提高产品安全性，我们强烈建议您根据如下规则设置较为复杂的密码：密码长度应在 8~16 位字符之间，由数字、小写字母、大写字母及特殊字符中四选二种以上类型组合而成。注：密码设置不可包含用户名。
- 建议系统管理员对用户权限进行有效管理，及时删除无关用户和权限。
- 管理员登录系统后及时绑定证书，进行账户安全设置，修改初始密码。

说明

- 系统中管理员和非管理员用户的用户名不可修改。管理员账号不可删除。
- 设置密码长度需达到 8~16 位，且至少由数字、小写字母、大写字母和特殊字符的两种或两种以上类型组合而成。
- 密码强度规则如下：
- 如果设置的密码包含三种或三种以上类型（数字、小写字母、大写字母、特殊字符），属于强密码。
- 如果设置的密码为数字和特殊字符组合、小写字母和特殊字符组合、大写字母和特殊字符组合、小写字母和大写字母组合中的一种，属于中密码。

- 如果设置的密码为数字和小写字母组合、数字和大写字母组合，属于弱密码。

为更好的保护您的隐私并提升产品安全性，建议您将风险密码更改为高强度密码。

3.4.2 用户修改

选择“配置→系统→用户管理”，进入用户管理界面，选择要修改的用户，点击“修改”按钮，弹出用户修改界面，修改相关信息。密码设置规则请参见添加用户的步骤。如图 3-8 所示。

图 3-8 用户修改

说明

账号安全设置：安全问题是防止管理员密码或者密码被盗取后，找回密码的验证问题。由您自己选定的三个问题，自己设置答案，当密码遗失或用户被盗找回密码时，可以填写密保问题，进一步找回密码。密保的范围是您的个人私有信息，其他人无法回答。

3.4.3 用户删除

管理员选择“配置→系统→用户管理”，选择要删除的用户，单击“删除”，提示“是否删除该用户？”，单击“确定”，该用户被删除。单击“取消”，提示“已取消删除”。不可删除管理员用户。如图 3-9 所示。

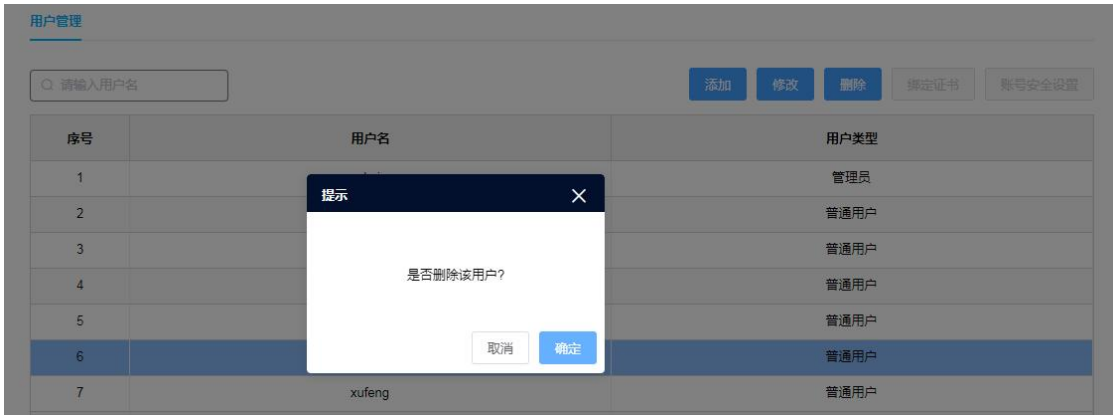


图 3-9 用户删除

4. 设备

设备管理用于管理所有接入服务系统的前端视频设备，设备管理界面显示信息包括设备名称、IP 地址、管理端口、安全性、证书状态、设备状态、协议类型和传输协议。界面如图 4-1 所示。

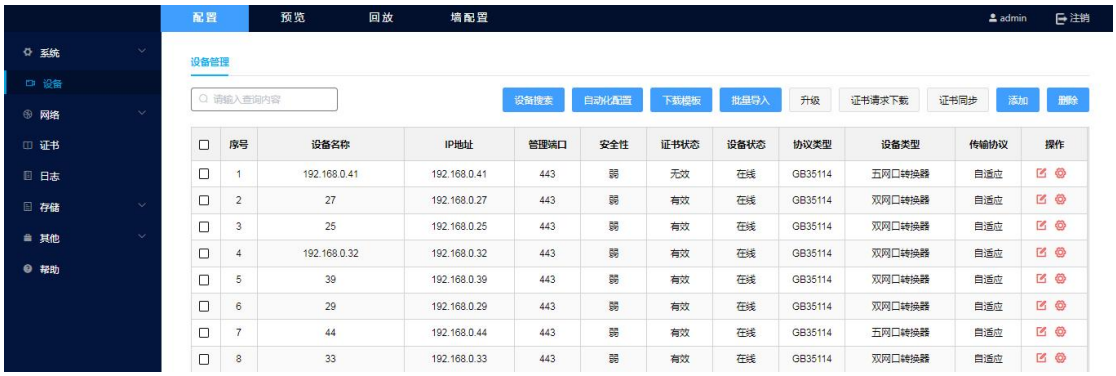


图 4-1 设备管理

4.1 设备添加

选择“配置→设备”，进入设备管理界面，单击“添加”，在设备添加界面输入设备信息，界面如图 4-2 所示。

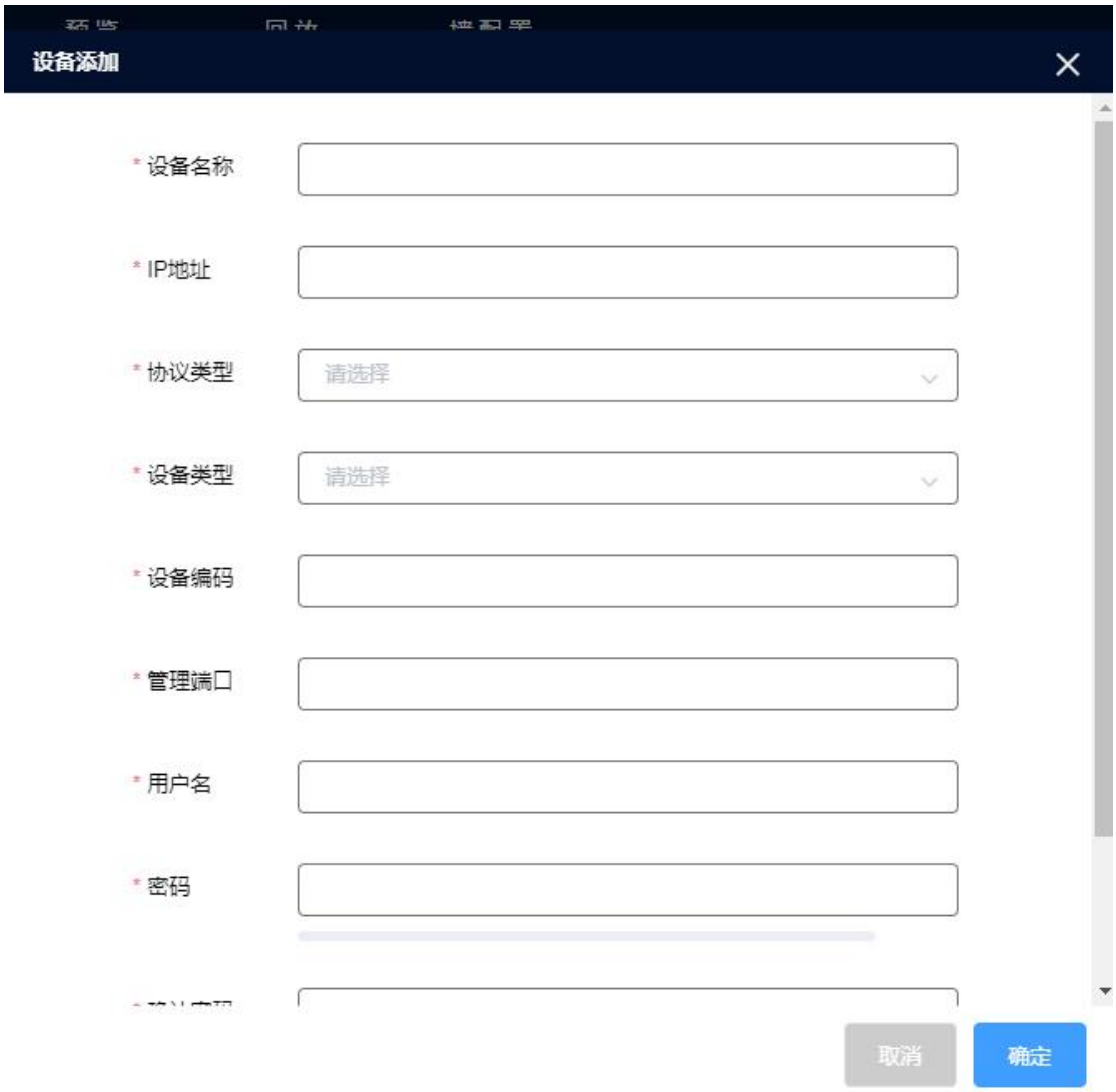


图 4-2 设备添加

说明

（1）设备名称：该设备名称为用户自定义。

（2）IP 地址：所添加的视频前端设备的 IP 地址。

（3）协议类型：支持 GB35114、GB28181、ONVIF、RTSP 设备的接入。

（4）设备类型：支持双网口安全转换器、五网口安全转换器和网络摄像机。

（5）设备编码：该设备编号为用户自定义（20 位数字）。

（6）管理端口：安全转换器在服务系统的登录端口号，默认为“443”。

（7）用户名、密码：用户访问视频安全转换器的用户名、密码。

（8）确认密码：用户需再次确认一遍登录该设备的密码。

（9）传输协议：支持 UDP、TCP 和自适应。

添加完成并提交后，该设备将出现在设备列表中，当完成证书配置后，该设备的证书状态会显示“有效”，在完成设备的所有配置正常工作后，设备状态会显示“在线”。

4.2 设备修改

单击设备操作列 “ ” 按钮，弹出设备修改界面，可修改设备名称，其他字段填写错误时不可修改，需删除重新添加。界面如图 4-3 所示。

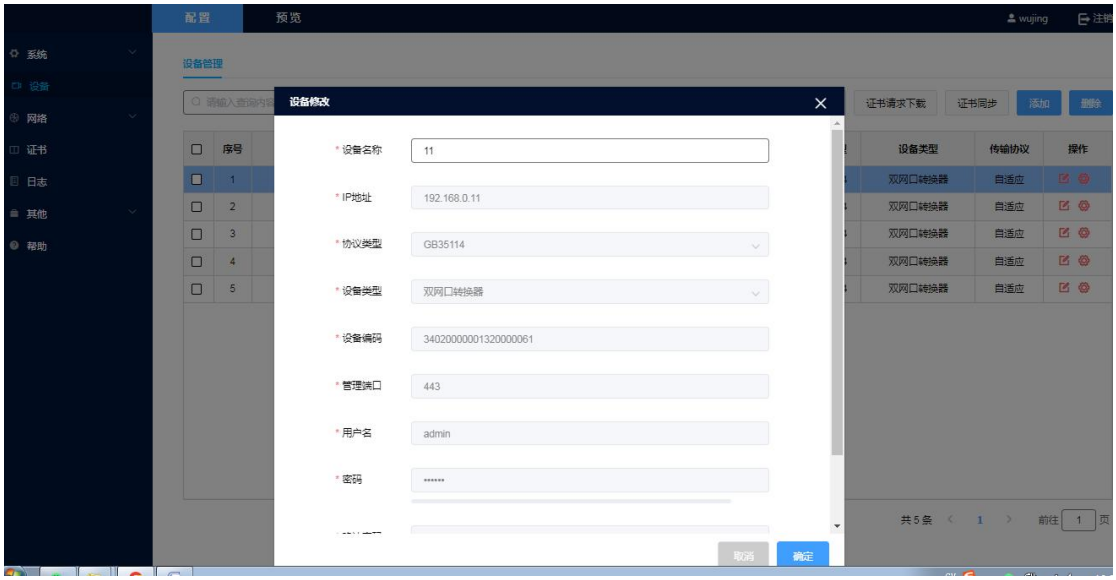


图 4-3 设备修改

4.3 设备远程控制

单击设备操作列远程控制按钮 “ ”，可进入前端安全转换器配置界面，详见“视频安全加固终端配置操作手册”。界面如图 4-4 所示。

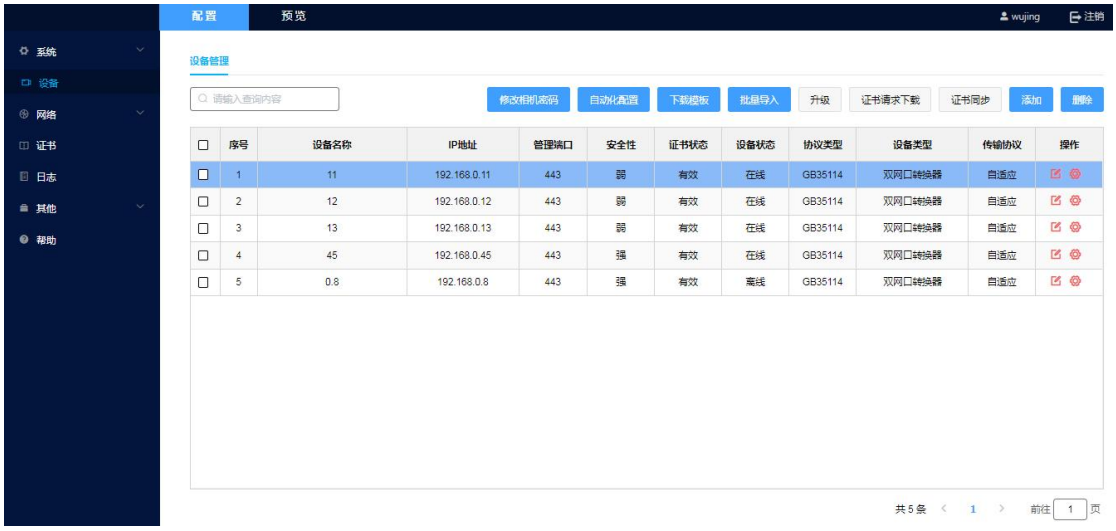


图 4-4 远程控制

4.4 设备证书操作

设备证书操作包括证书请求下载和证书同步。证书类型为 GB35114 协议可下载同步证书请求。界面如图 4-5 所示。

图 4-5 设备证书操作

说明

“证书请求下载”：至少选择一个设备，单击“证书请求下载”形成设备证书签发请求，可在“证书-证书签发”中点击响应。

“证书同步”：选择要同步的证书，单击“证书同步”后可将证书同步到设备端，可进行多个设备同步证书。界面如图 4-6 所示。

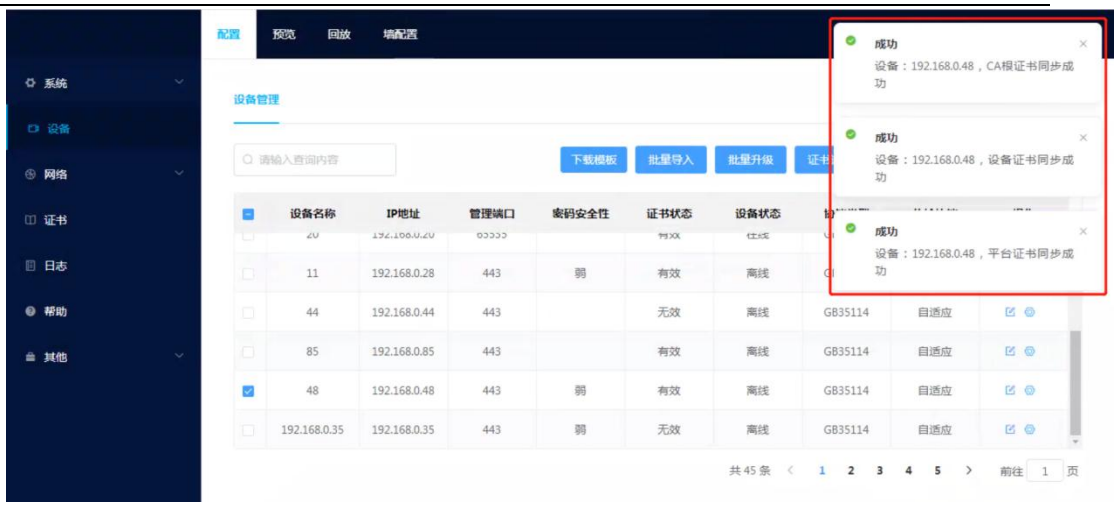


图 4-6 证书同步

4.5 设备删除

选择要删除的设备，单击“删除”按钮，提示“是否删除该设备？”，单击“确定”按钮，选中的设备从设备列表中移除。单击“取消”按钮，提示“已取消删除”。界面如图 4-7 所示。

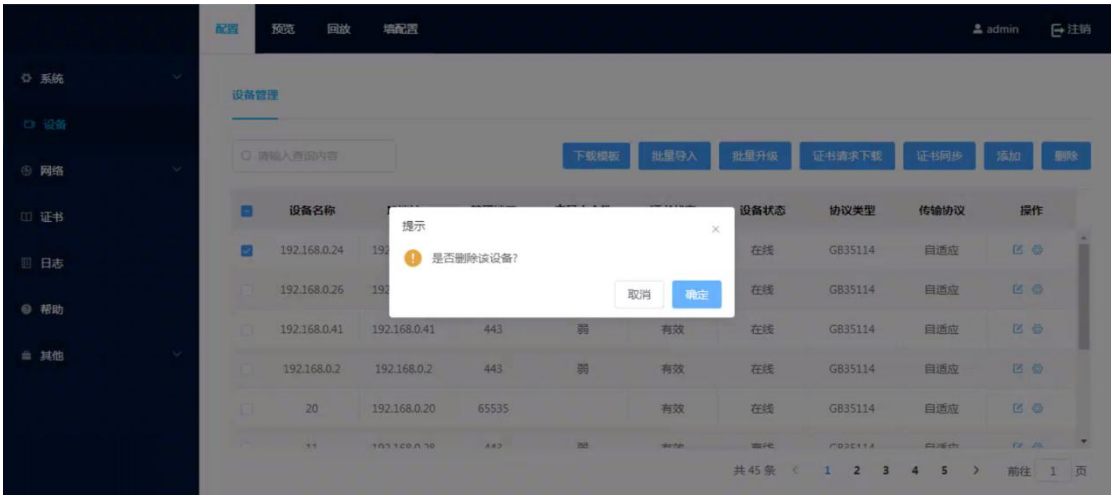


图 4-7 设备删除

4.6 下载模板

单击“下载模板”，将设备批量添加模板下载至本地计算机中。界面如图 4-8 所示。

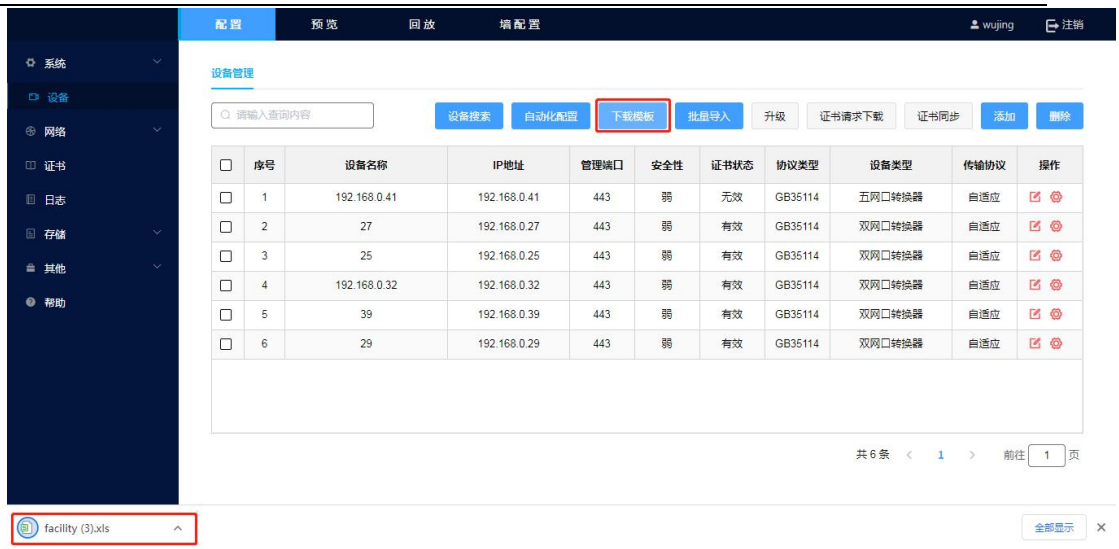


图 4-8 下载模板

注意

模板数据如图 4-9 所示。数据维护时需注意：

（1）设备名称不能重复。

（2）IP 地址和管理端口组合不能重复。

（3）协议类型可选择 GB35114、GB28181、ONVIF 或 RTSP。

（4）协议类型为 RTSP 时，主流码必填，子流码非必填。协议类型为 GB35114、GB28181、ONVIF 时，除主流码和子流码，其他字段为必填项。

（5）设备类型可选择双网口转换器、五网口转换器或 IPC。

（6）传输协议可选择自适应、UDP、TCP。

图 4-9 设备批量导入模板

4.7 批量导入

根据下载模板的注意事项在模板中维护数据并保存。

单击“批量导入”，选择文件可将模板中数据导入到设备列表中。数据维护正确时，设备列表自动展示导入的数据。如图 4-10 所示。

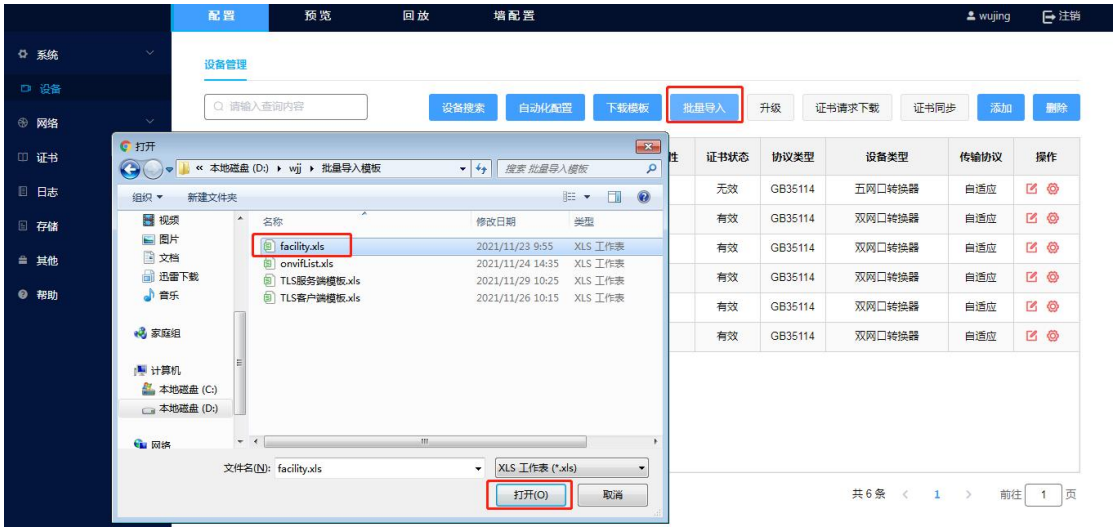


图 4-10 批量导入

导入时检验数据正确性，可根据添加失败数据界面的行号和错误详情修改数据，修改正确后导入。如图 4-11 所示。

图 4-11 添加失败数据

4.8 设备自动化配置

可对单个设备或多个设备平台接入数据批量配置。批量创建证书，同步证书，同时启用平台接入功能。界面如图 4-12 所示。

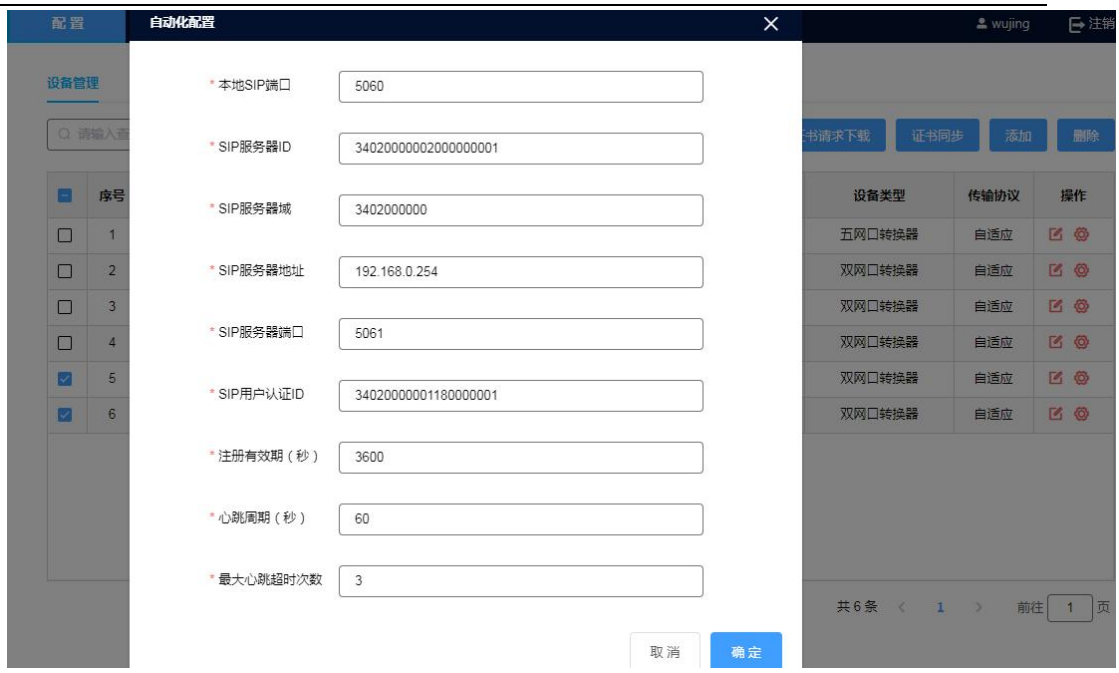


图 4-12 设备自动化配置

4.9 批量升级

可对单个设备或多个设备进行升级。选中需要升级的设备，单击“升级”，选择升级文件。如图 4-13 所示。

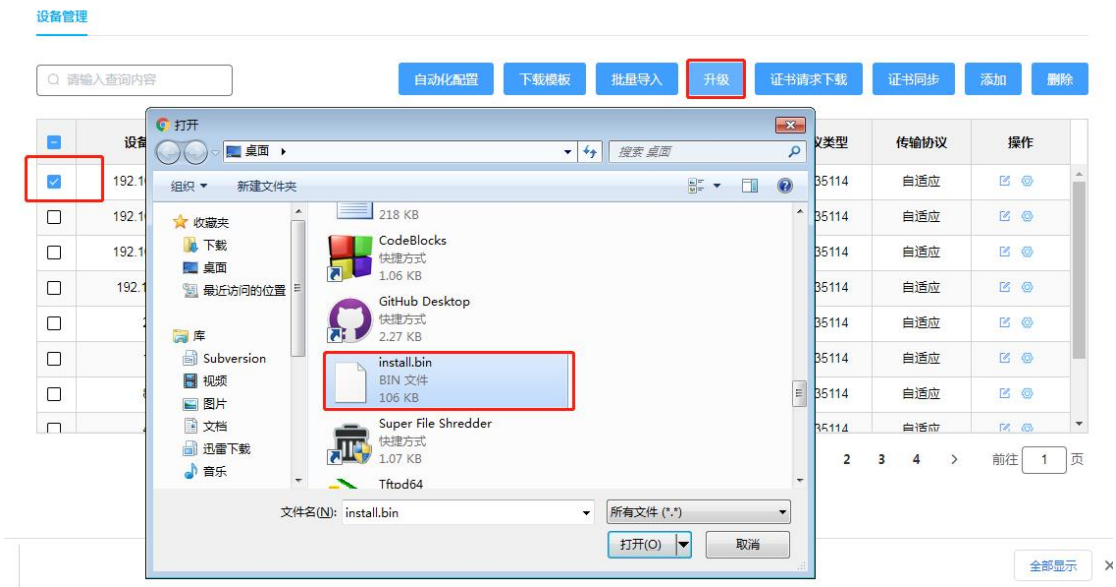


图 4-13 设备批量升级

4.10 批量修改相机密码

可对单个设备或多个设备接入的前端相机的登录密码批量修改。

选中需要修改接入相机的设备，单击“修改相机密码”， 弹出修改相机密码界面，可根据接入的通道修改对应相机密码。修改完成后需单击“确定”。完成批量修改密码功能。如图 4-14 所示。

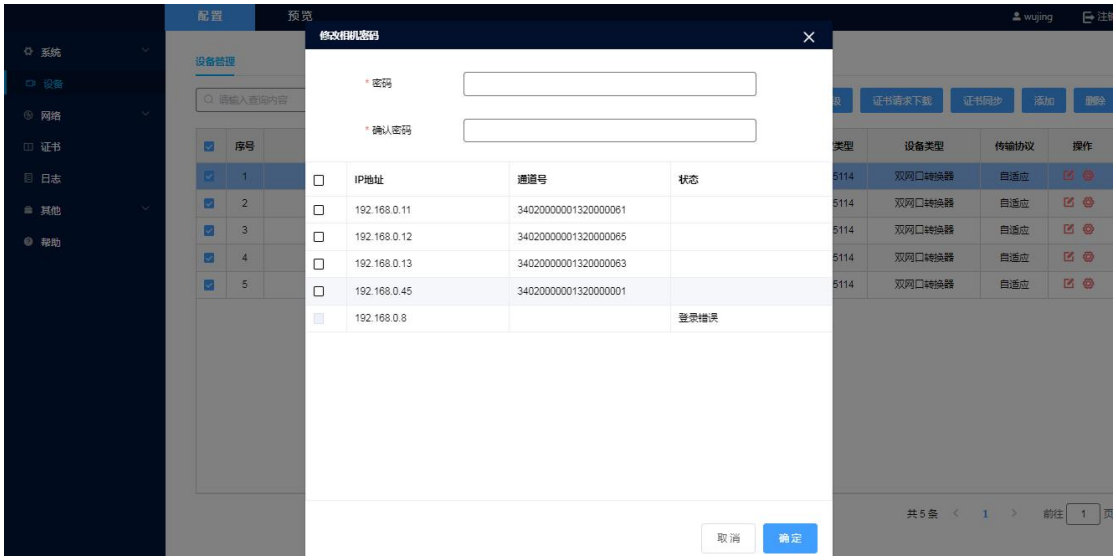


图 4-14 批量修改相机密码

5. 网络配置

选择“配置→网络”，进入网络配置，网络配置包括基本配置、高级配置等内容。

5.1 基本配置

选择“配置→网络→基本配置”，基本配置包括 TCP/IP 配置和端口配置。

TCP/IP 配置视频安全服务系统的网络，网卡类型默认自适应，设备 IPv4 地址、IPv4 默认网关、IPv4 子网掩码、首选 DNS 服务器、备用 DNS 服务器可修改。

端口配置包括 RTSP 端口和 HTTPS 端口。

以上配置如有修改，需单击“保存”。提示“保存成功”。界面如图 5-1 所示。

图 5-1 基本配置

5.2 高级配置

视频设备安全服务平台支持 GB/T28181 和 GB 35114 两种协议的转换。安全一体机融合国密安全芯片支持 GB 35114 协议要求，前端摄像机可通过 GB/T28181 协议接入安全加固终端，由安全加固终端完成 GB/T 28181 向 GB35114 的协议转换，并连入上级 35114 视频安全服务平台。

5.2.1 平台接入

（1）平台接入方式为 GB/T28181，应与上级视频业务平台接入协议一致。

（2）本地 SIP 端口：本级视频信息安全一体机向上级视频业务平台进行 SIP 信令通信的端口号，默认 5060，范围 1025-65535。

（3）SIP 服务器 ID：接入上级视频业务平台的目的 SIP 服务器 ID，20 位数

字。

（4）SIP 服务器域：视频信息安全一体机的 SIP 域编号，为 SIP 服务器 ID 的前 10 位。

（5）SIP 服务器地址：接入上级视频业务平台的目的 SIP 服务器 IP 地址。

（6）SIP 服务器端口：接入上级视频业务平台的目的 SIP 服务器 28181 服务端口号，默认为“5060”，范围 1025-65535。

（7）SIP 用户认证 ID：本级视频信息安全一体机的 SIP 服务器编号，设备唯一标识。

（8）密码：视频信息安全一体机在视频业务平台中的注册密码。初始密码是 123456，可修改，注册密码写入即可，SIP 服务器调用。

（9）密码确认，再次输入密码，如输入和密码不一致，提示“两次输入密码不一致”。

（10）注册有效期（秒）：视频信息安全一体机注册到视频业务平台的有效期限。默认为“3600”，即设备 3600 秒内没有注册成功，表示本次注册失败，建议采用默认值，范围 100-100000。

（11）心跳周期（秒）：设备发送心跳信息的时间间隔。系统默认心跳周期为 60s，建议采用默认值，范围 5-3600。

（12）最大心跳超时次数：心跳信息连续超时达到“最大超时次数”，则认为视频安全服务系统无法与视频业务平台建立连接。系统默认最大超时次数为 3 次，建议采用默认值，范围 3-255。

界面如图 5-2 所示。

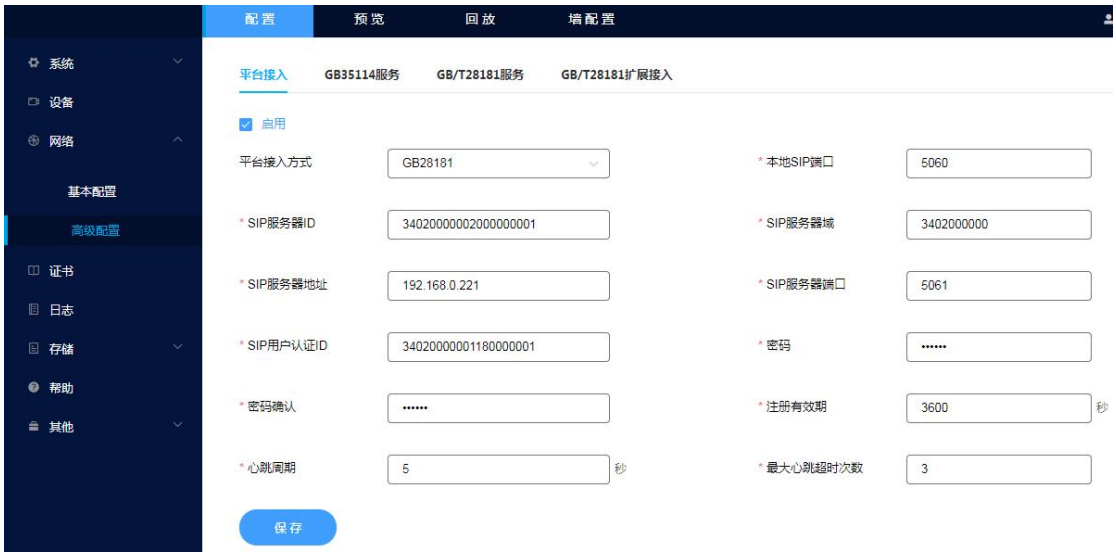


图 5-2 平台接入

5.2.2 GB35114 服务

（1）启用 GB35114 服务前需先完成证书配置。

（2）SIP 服务器 ID：本级视频安全服务系统的 SIP 服务器编号，设备唯一标识。

（3）SIP 服务器端口：本级视频安全服务系统 35114 服务端口。

（4）最大心跳超时次数：心跳信息连续超时达到“最大超时次数”，则认为安全加固终端无法与视频安全服务系统建立连接。系统默认最大超时次数为 3 次，建议采用默认值，范围 3-255。

（5）心跳周期（秒）：设备发送心跳信息的时间间隔。系统默认心跳周期为 60s，建议采用默认值，范围 5-3600。

界面如图 5-3 所示。

图 5-3 GB35114 服务

（6）证书管理功能用于管理平台证书。

单击“创建证书请求-创建”按钮，创建平台证书，证书请求的基本信息显示在按钮右边。

单击“证书请求下载-下载”按钮，可将证书请求的 CSR 文件下载到本地。

单击“证书请求删除-删除”按钮，创建的证书请求被删除。

界面如图 5-4 所示。

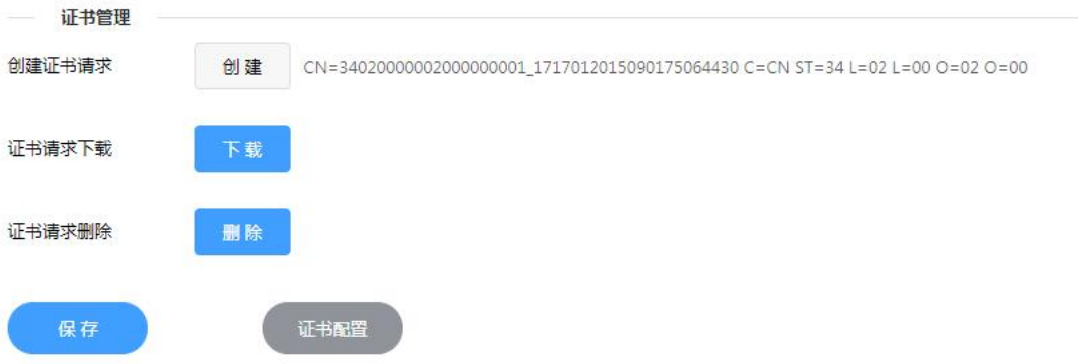


图 5-4 证书管理

（7）勾选自动添加 IPC，将 35114 协议的前端设备直接接入视频安全一体机系统中。

5.2.3 GB/T28181 服务

启用接入 GB/T28181 服务：

（1）SIP 服务器 ID：本级视频安全服务系统的 SIP 服务器编号，设备唯一标识。

（2）SIP 服务器端口：本级视频安全服务系统 35114 服务端口。

（3）密码：视频安全服务系统在视频业务平台中的注册密码。初始密码 123456，可修改，注册密码写入即可，SIP 服务器调用。

（4）密码确认：再次输入密码，如密码确认和密码输入不一致，提示“两次输入密码不一致”。

（5）心跳周期：设备发送心跳信息的时间间隔。系统默认心跳周期为 60 秒，建议采用默认值，范围 5-3600。

（6）最大心跳超时次数：心跳信息连续超时达到“最大超时次数”，则认为视频安全服务系统无法与视频业务平台建立连接。系统默认最大超时次数为 3 次，建议采用默认值，范围 3-255。

（7）勾选自动添加 IPC，将 28181 协议的前端设备直接接入视频安全一体机系统中。

以上配置信息如有修改，需单击“保存”，提示“保存成功”。界面如图 5-5 所示。

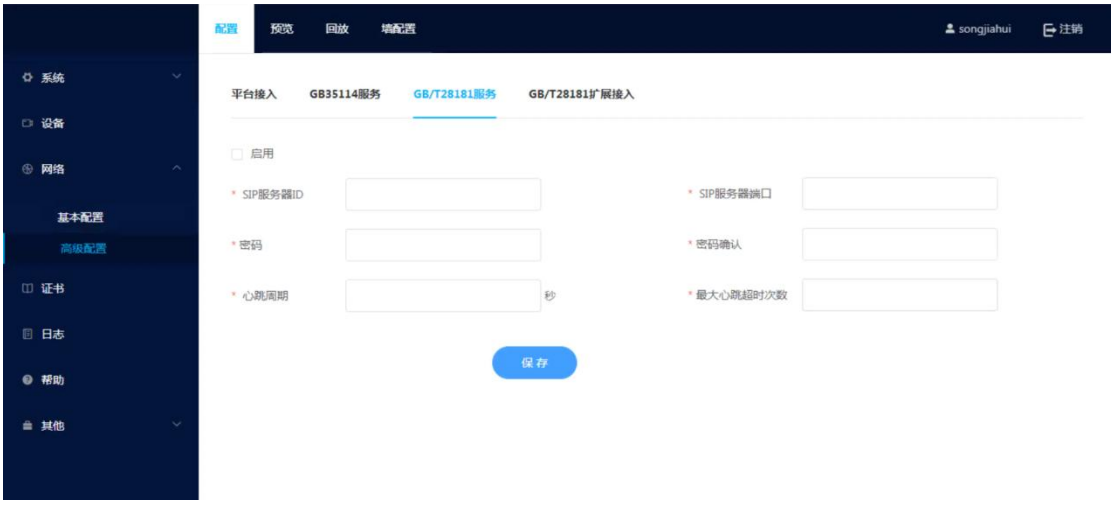


图 5-5 GB/T28181 服务

5.2.4 GB/T28181 扩展接入

（1）平台接入方式为 GB/T28181，不可修改。

（2）SIP 服务器 ID：接入上级视频业务平台的目的 SIP 服务器 ID，20 位数字。

（3）SIP 服务器域：视频安全系统的 SIP 域编号，为 SIP 服务器 ID 的前 10 位。

（4）SIP 服务器地址：接入上级视频业务平台的目的 SIP 服务器 IP 地址。

（5）SIP 服务器端口：接入上级视频业务平台的目的 SIP 服务器 28181 服务端口号，默认为“5060”，范围 1025-65535。

（6）密码：视频安全服务系统在视频业务平台中的注册密码。初始密码是 123456，可修改。

（7）密码确认：再次输入密码，如密码确认和密码输入不一致，提示“两次输入密码不一致”。

（8）注册有效期：视频安全服务系统注册到视频业务平台的有效期限。默认为“3600”，即设备 3600 秒内没有注册成功，表示本次注册失败，建议采用默认值，范围 100-100000。

（9）心跳周期：设备发送心跳信息的时间间隔。系统默认心跳周期为 60 秒，建议采用默认值，范围 5-3600。

（10）最大心跳超时次数：心跳信息连续超时达到“最大超时次数”，则认为视频安全服务系统无法与视频业务平台建立连接。系统默认最大超时次数为 3 次，建议采用默认值，范围 3-255。

界面如图 5-6 所示。

图 5-6 GB/T28181 扩展接入

（11）平台接入配置信息

获取 GB/T28181 配置界面的 SIP 服务器地址和 SIP 服务器 ID。

单击“保存”，保存当前配置的 GB/T28181 扩展接入数据。

单击“添加”，新增 GB/T28181 扩展接入输入界面，配置数据完成后单击当前行对应的“保存”保存配置数据。

单击当前行对应的“移除”删除当前配置数据。界面如图 5-7 所示。

图 5-7 平台接入配置信息

（12）视频通道编码配置信息

选中平台接入配置信息某一行，单击视频通道编码配置信息页签，配置 GB/T28181 扩展接入的视频通道 ID。

单击“添加”显示视频安全服务系统接入的前端视频通道编码 ID，可单选可多选视频通道编码 ID。选择完成后显示在视频通道编码配置信息页签中。

单击“移除”，删除当前 SIP 服务器 ID 关联的视频通道编码。界面如图 5-8 所示。

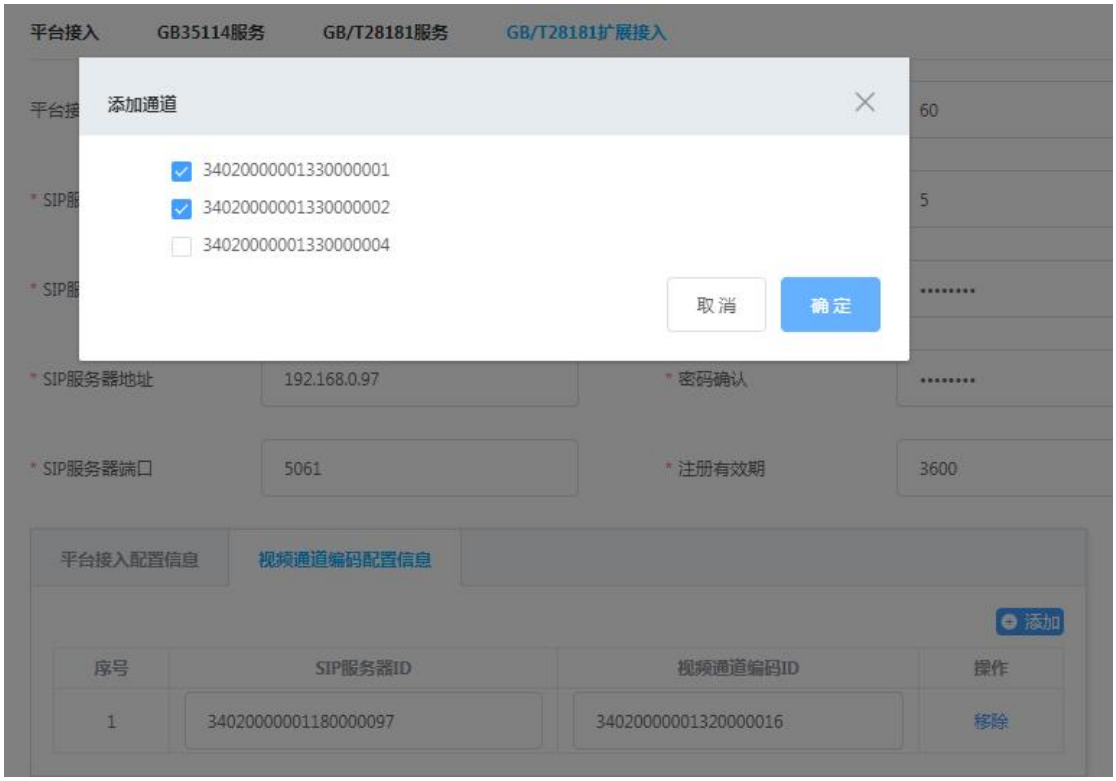


图 5-8 视频通道编码配置

5.2.5 资源配置

流媒体服务的主要功能是进行音视频流的转发、复制转发等。通过添加或删除流媒体服务器实现对流媒体的管理。界面如图 5-9 所示。

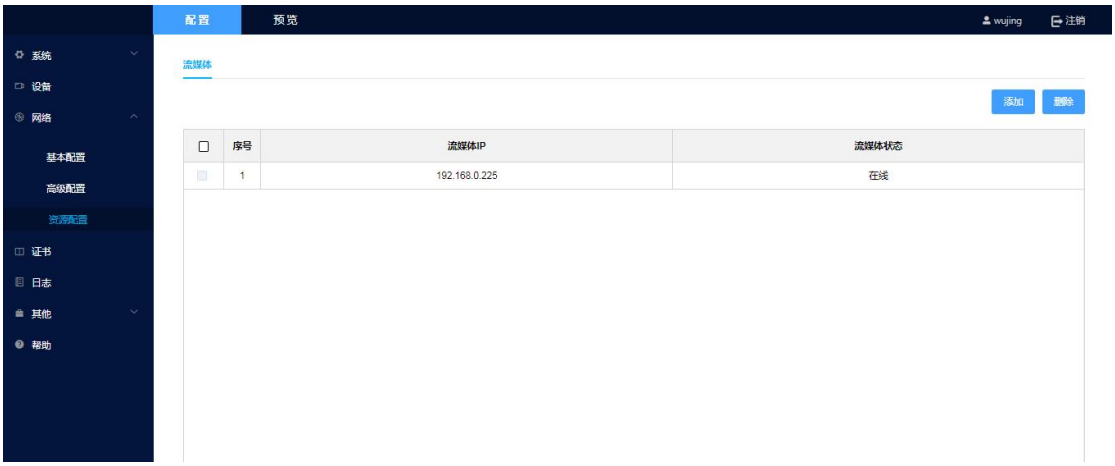


图 5-9 资源配置

（1）流媒体添加

选择“网络→资源配置”，进入资源配置界面，单击“添加”，弹出添加流媒体数据界面，如图 5-10 所示。

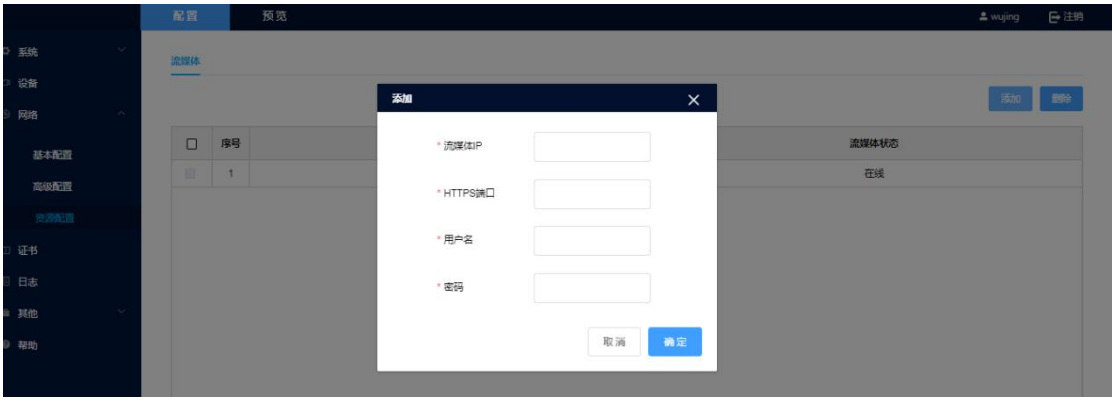


图 5-10 添加流媒体

说明

流媒体 IP：所添加流媒体的 IP 地址。

HTTP 端口：所添加流媒体的 HTTP 端口。

用户名：访问流媒体的用户名。

密码：访问流媒体的密码。

（2）流媒体删除

选择“网络→资源配置”，进入资源配置界面，选择一个或多条流媒体数据，单击“删除”， 提示“是否删除？”，单击“确定”按钮，选中的流媒体信息从资源配置列表中移除。单击“取消”按钮，提示“已取消删除”。界面如图 5-11 所示。

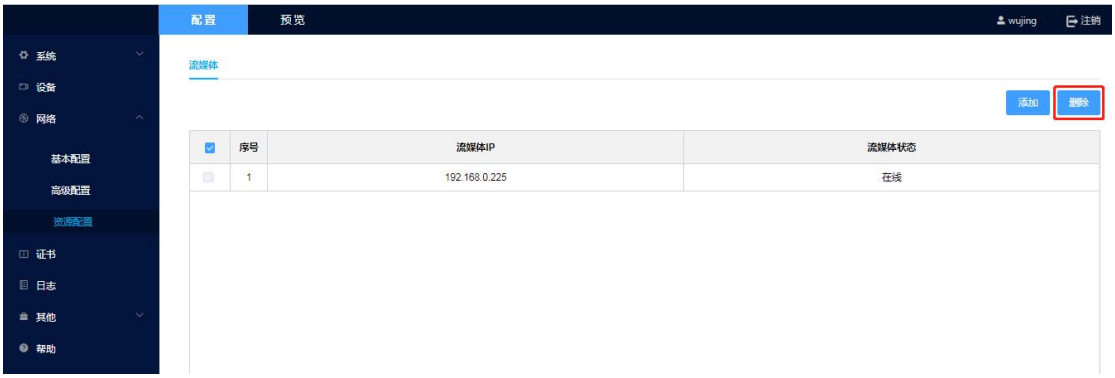


图 5-11 删除流媒体

6. 证书

6.1 证书管理

证书管理包括证书序列号、签发者、证书主体信息、证书主体 CN 信息、失效日期、证书类型、证书状态。

（1）证书序列号是证书唯一识别码。

（2）签发者是证书签发者的 CA 身份标识。

（3）设备主体信息是该证书所属设备的 SIP 服务器 ID 和设备密码模块的编号。

（4）失效日期是证书失效的日期，记录到年月日时分秒。

（5）证书类型包括根证书、平台证书和设备证书。

（7）证书状态分为正常、已冻结、已过期。

正常状态为证书正常使用中；冻结状态为因发现证书的异常状态，而冻结证书使之暂时无法正常使用，由安全操作员操作证书的冻结和解冻；过期状态表示证书已过有效日期或由于安全原因不再使用，应进行删除操作，此时被删除证书将加入撤销列表中。界面如图 6-1 所示。

图 6-1 证书管理

6.1.1 证书下载

进入“证书→证书管理”查看签发的证书信息，选择一条或多条证书信息，单击“下载”，下载证书 CER 文件。界面如图 6-2 所示。

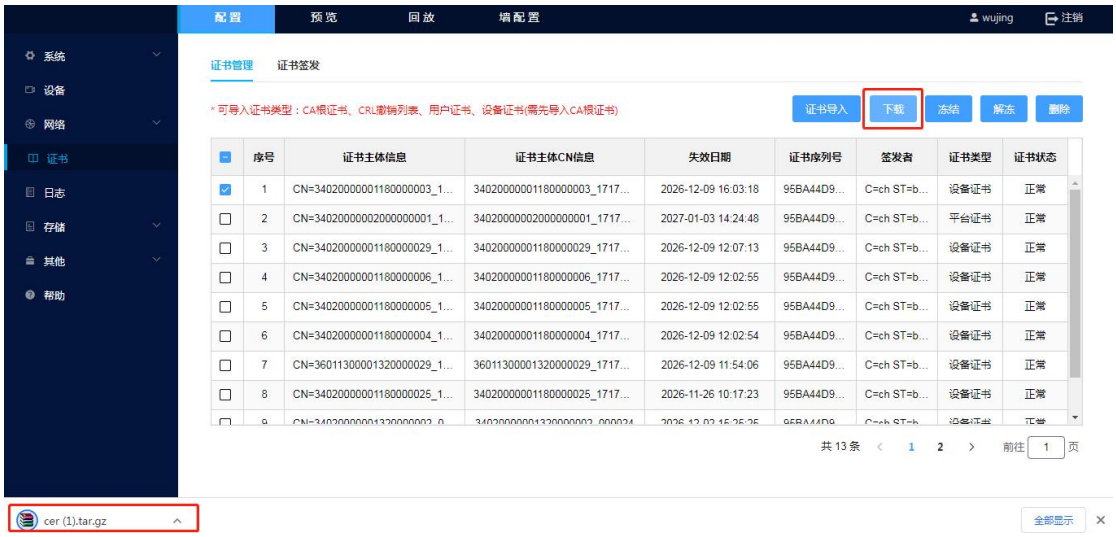


图 6-2 证书下载

6.1.2 证书冻结/解冻

（1）证书冻结

进入“证书→证书管理”查看签发的证书信息，选择一条或多条证书信息，单击“冻结”，证书列表中证书状态为冻结。设备证书状态为冻结时，此时“设备→设备管理”中证书状态变为“无效”。界面如图 6-3 所示。

注：CA 根证书不能进行冻结操作。

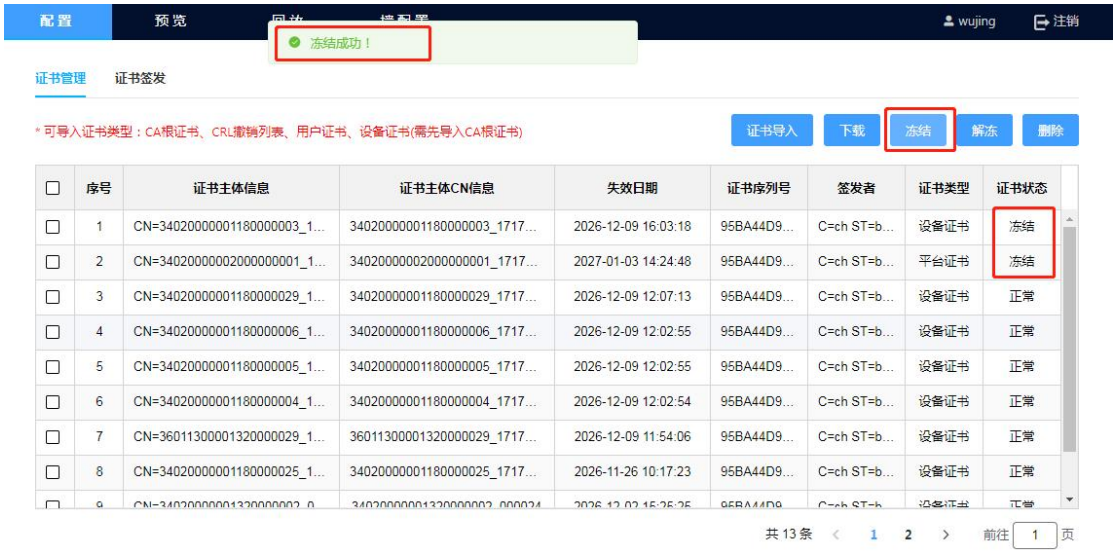


图 6-3 证书冻结

（2）证书解冻

选择证书状态为“冻结”的设备证书或者平台证书，单击“解冻”，证书列

表中证书状态为“正常”。此时“设备→设备管理”中证书状态变为“有效”。界面如图 6-4。

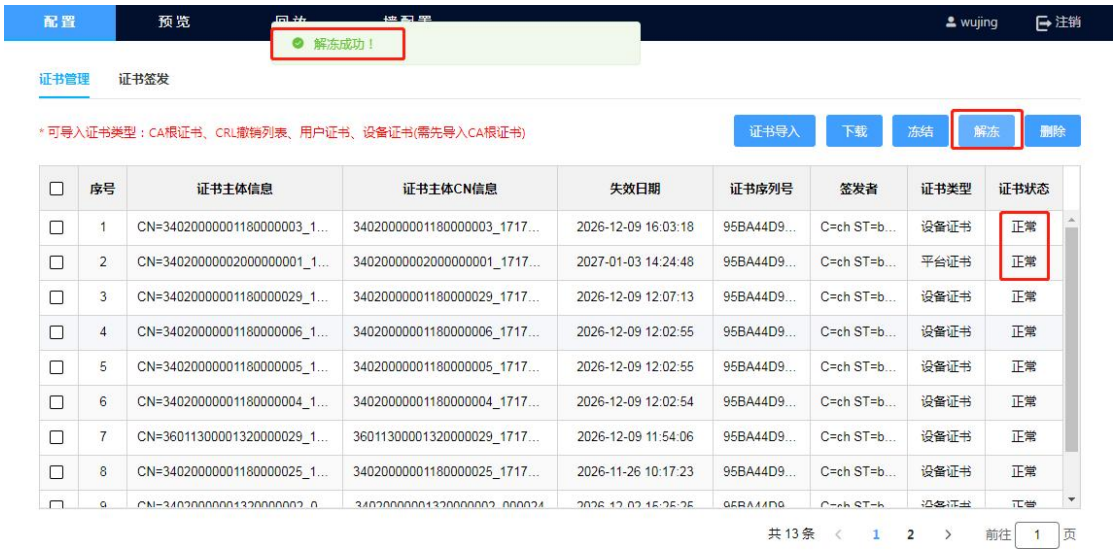


图 6-4 证书解冻

6.1.3 证书删除

进入“证书→证书管理”查看签发的证书信息，选择一条或多条证书信息，单击“删除”，系统提示“确认删除”，单击“确定”，提示“证书删除成功”，删除的证书信息不在证书管理界面显示。证书删除后，“设备→设备管理”中设备对应的证书状态变为“无效”。界面如图 6-5 所示。

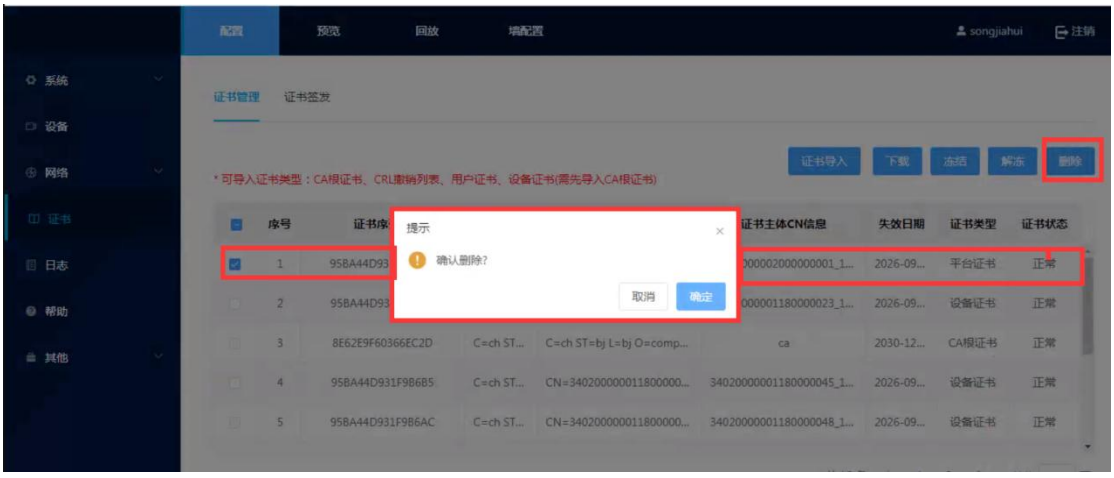


图 6-5 证书删除

6.2 证书签发

证书签发包括申请证书类型、有效期（天）、申请时间、申请信息。证书签

发操作有下载、签发、删除功能。

（1）申请证书类型包括根证书、平台证书和设备证书。

（2）有效期为证书签发请求的有效期，默认为 1800 天。

（3）申请时间为发起证书签发请求的时间，记录到年月日时分秒。

（4）申请信息为证书请求信息的用户标识。

（5）签发操作

单击“签发”签发成功后签发出的证书信息会展示在证书管理页面中，同时该条签发请求信息会在证书签发列表中清除；选择一条或多条签发请求，单击“删除”，选择的证书签发请求会被删除。界面如图 6-6 所示。

图 6-6 证书签发

6.3 在线导入

6.3.1 根证书

根证书为产品出厂预置，登录完成后，可在“证书→证书管理”中查看根证书相关信息。界面如图 6-7 所示。

图 6-7 根证书

6.3.2 平台证书创建/签发

在“网络→高级配置→GB35114 服务→证书管理→创建证书请求”，单击“创建”，创建按钮后显示平台证书信息。

单击“证书配置”跳转至“证书→证书管理”，单击“证书签发”，证书签发页面显示平台证书的签发请求。也可以直接进入“证书→证书签发”，单击“签发”签发成功后可在“证书→证书管理”中查看平台证书的相关信息；如果发生证书更新，再次签发，需先删除上次创建的证书请求，再重复此流程。界面如图 6-8、6-9 所示。

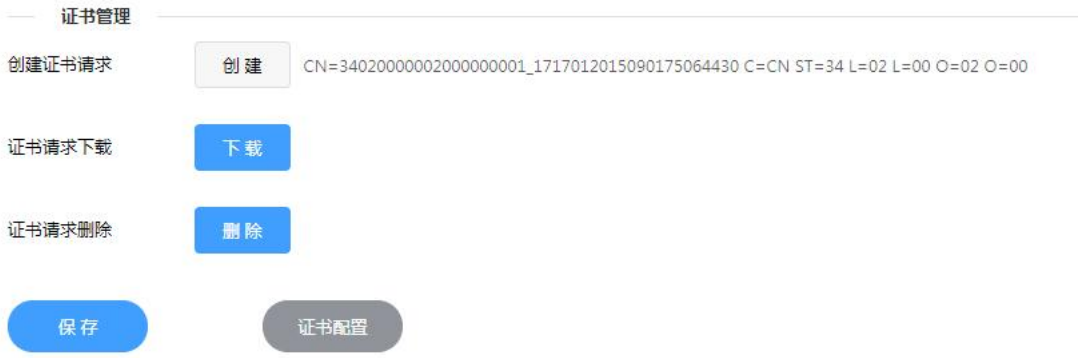


图 6-8 平台证书创建

图 6-9 平台证书签发

6.3.3 设备证书创建/签发

（1）设备添加成功后，进入“设备→远程控制→网络→高级配置→证书管理”，单击“创建证书请求-创建”，完成后关闭远程控制页面。界面如图 6-10、6-11 所示。

图 6-10 远程控制

图 6-11 设备证书创建

（2）在“设备→设备管理”中选择设备，单击“证书请求下载”，页面提示示“设备 192.XX.XX.XX，证书下载成功”。界面如图 6-12 所示。

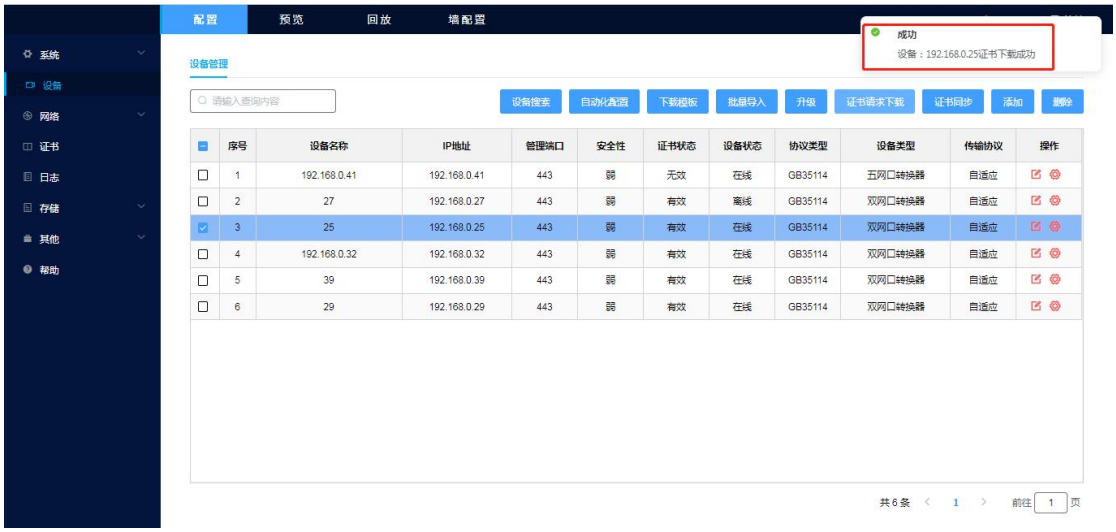


图 6-12 证书下载成功

（3）在“证书→证书签发”中发现设备证书签发请求。选择该条请求，单击“签发”，签发成功后可在“证书→证书管理”中查看设备证书的相关信息；如果发生更新，再次签发证书，需先删除上次创建的证书请求，再重复此流程。

界面如图 6-13、6-14 所示。

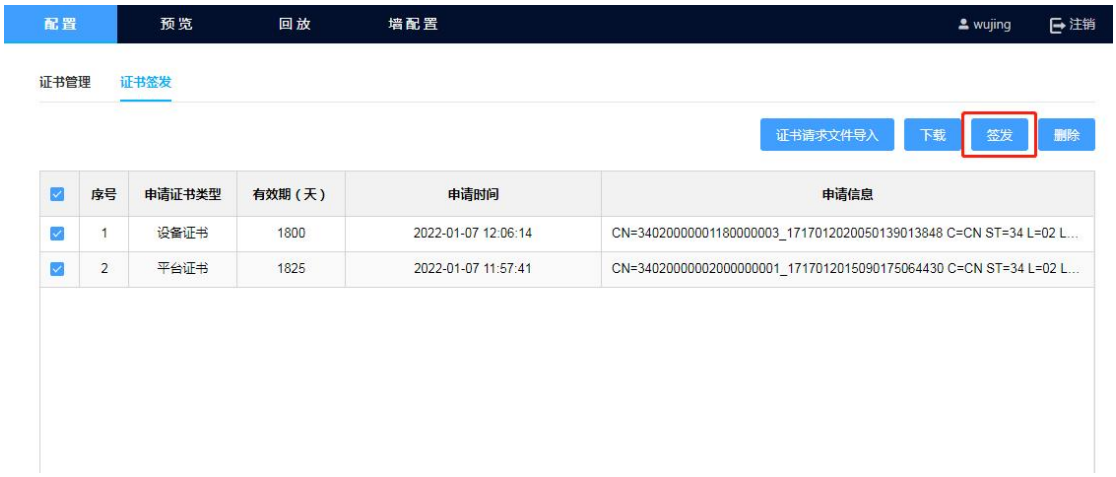


图 6-13 证书签发

图 6-14 证书导入

6.3.4 证书同步

在“设备→设备管理”中，选择要证书同步的设备，页面提示“设备：192.XX.XX.XX，CA 证书同步成功”、“设备：192.XX.XX.XX，设备证书同步成功”、“设备：192.XX.XX.XX，平台证书同步成功”则完成证书同步操作。界面如图 6-15 所示。

图 6-15 证书同步

6.4 离线导入

6.4.1 平台证书文件下载/删除

在“网络→高级配置→GB35114 服务→证书管理”中，单击“创建证书请求”，

单击“下载”，将创建的证书请求下载到本地计算机当中，生成一个 CSR 文件，用户需要将 CSR 文件发送给 CA 认证中心进行平台证书签发；如果发生更新，再次签发证书，需单击“删除”，删除上次创建的证书请求，再重复此流程。

界面如图 6-16 所示。

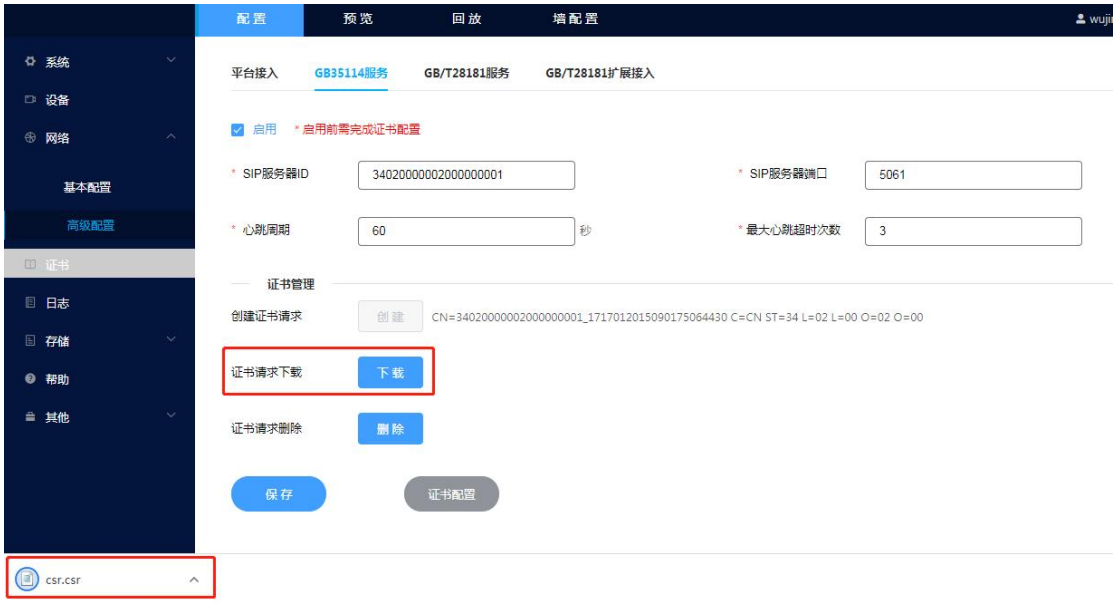


图 6-16 平台证书请求下载

6.4.2 设备证书文件下载/删除

设备添加成功后，进入该设备的“远程控制→网络→高级配置→证书管理”中，单击“创建证书请求”，单击“下载”，将创建的设备证书请求下载到本地计算机当中，生成一个 CSR 文件，用户需要将 CSR 文件发送给 CA 认证中心进行设备证书签发；如果发生更新，再次签发证书，需单击“删除”，删除上次创建的证书请求，再重复此流程。

界面如图 6-17 所示。

图 6-17 设备证书请求下载

6.4.3 证书离线导入/签发

用户从 CA 认证中心获取生成的平台证书和设备证书的 CER 文件，在证书管理界面单击“证书导入”将平台证书和设备证书的 CER 文件导入系统，可在证书管理界面查看导入的平台证书和设备证书。界面如图 6-18 所示。

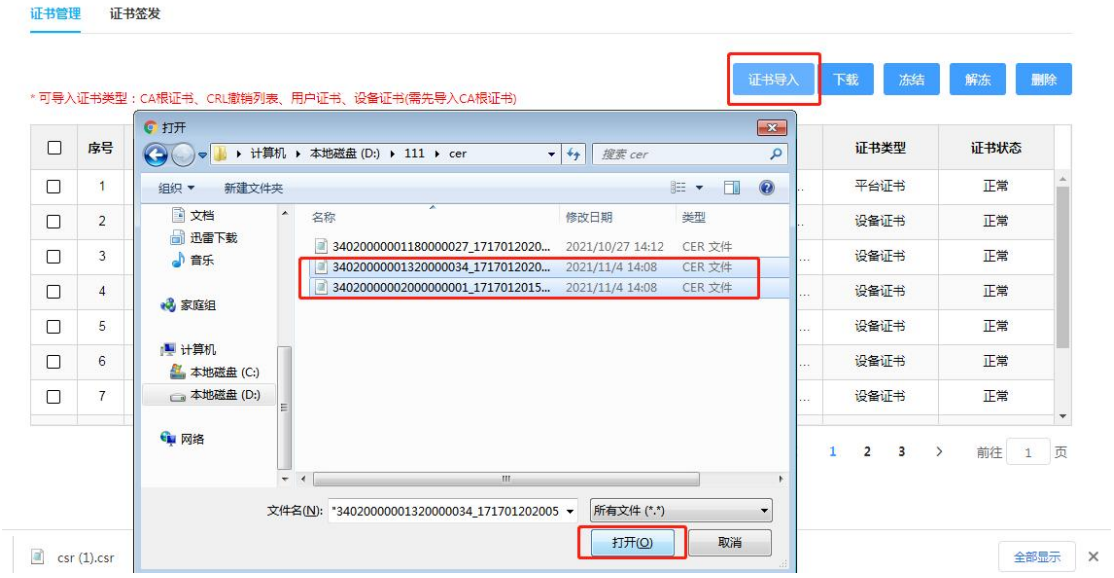


图 6-18 证书导入

6.4.4 证书同步

在“设备→设备管理”中，勾选对应设备，点击“证书同步”，页面提示“设备：192.XX.XX.XX，CA 证书同步成功”、“设备：192.XX.XX.XX，设备证书同步成功”、“设备：192.XX.XX.XX，平台证书同步成功”则完成证书同步操作。

界面如图 6-19 所示。

图 6-19 证书同步

7. 录像预览

视频预览可浏览接入前端摄像机的视频。预览视频可进行单屏预览和多屏预览（最多可支持四屏预览）。预览页面支持视频不加密预览、加密解密预览、视频截图、视频录制和全屏预览。界面如图 7-1、7-2 所示。

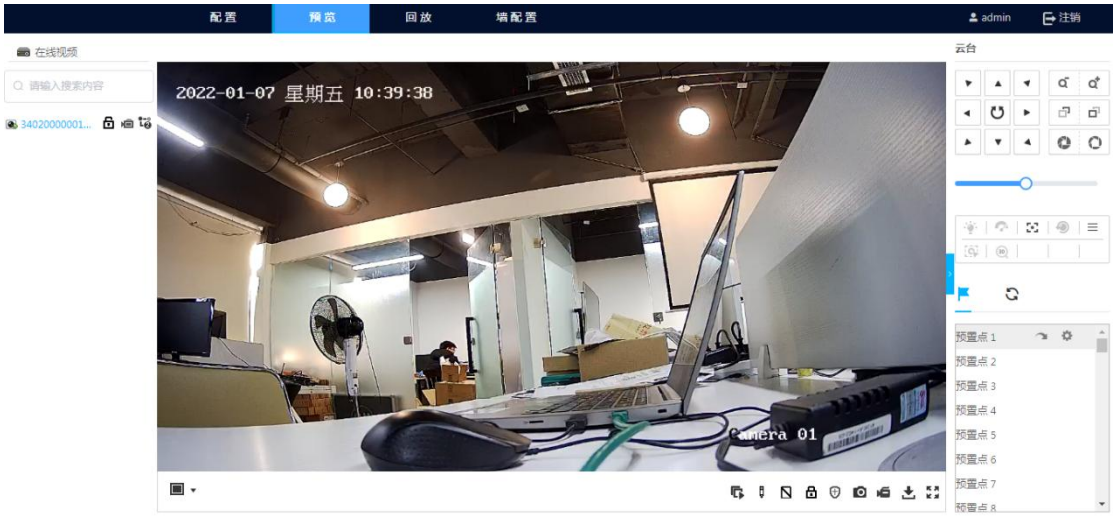


图 7-1 预览界面

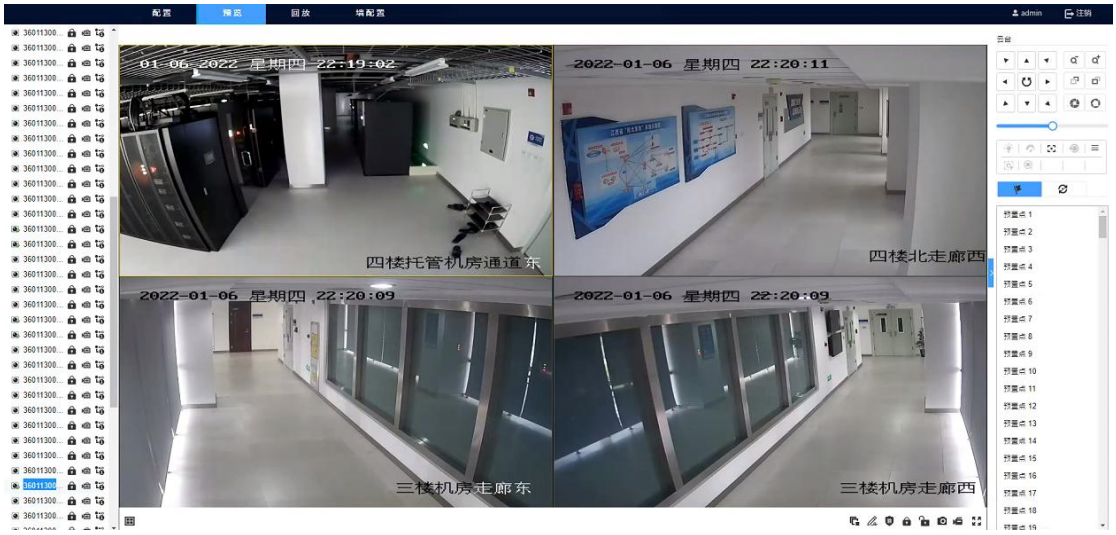


图 7-2 多屏预览

7.1 预览工具栏

视频预览：单击在线视频列表中任意一台设备，设备接入平台，画面播放区域显示监控画面。

图标	名称	功能说明
	全部开始预览	点击“全部开始预览”按钮，在线列表视频开始播放。再次点击，预览播放停止。
	画面布局	画面播放区域左下角的切换布局按钮，可单屏预览也可多屏预览。
/	签名/取消签名	对视频开启签名和取消签名。
/	验签/取消验签	对视频开启验签和取消验签
/	加密/取消加密	点击“加密”按钮，提示“加密成功！”，此时视频被加密，视频预览被暂停。按钮变为 ，再次点击，提示“取消加密成功！”，视频预览从当前时间继续播放。

/	开启解密	视频处于被加密状态下，点击“开始解密”按钮，提示“解密成功！”按钮变为“停止解密” 。视频预览从当前时间继续播放。在视频平台被解密的状态下，再次点击“停止解密”按钮，提示“取消解密”，平台停止对已加密视频流的解密工作，视频预览被暂停。
	抓图	可对预览窗口中的实时画面进行手动抓拍。点击“抓图”按钮，抓图为.png 的文件被下载。
	全部开启录像	首次单击开始录像，再次单击录像结束，并自动保存到已设置路径。录像文件“XX.gif”被下载。
	全屏	在全屏模式下显示实时视图。按 Esc 键，退出全屏模式。

7.2 云台控制

通过云台控制功能可以远程调整摄像机镜头的角度、焦距、光圈等，扩大摄像机监控范围，查看监控细节，从而实现全方位监控。同时支持设置预置点和巡航路径，方便用户查看指定监控方位的实时状况。

7.2.1 云台控制面板

图标	名称	功能说明
	云台控制按钮	可以通过预览窗口的云台控制方向图标，实现云台方向转动。云台将按箭头的方向转动，长按可以快速转动。选中任意一个正在播放的视频，点击任意方向的控制按键，相机会向着按

		钮对应的方向开始移动。
	调焦控制、调焦-/调焦+	用来调整镜头拍摄范围。 如果需要查看全景画面，建议适度缩小焦距；如需要查看近景视图或监控细节，建议适度放大焦距。
	聚焦控制 焦距-/焦距+	用来调整画面清晰度。如果要查看远距离的物体或场景，建议适当拉近焦距；如果要查看近距离的物体或场景，建议适当拉远焦点。
	速度控制	选中任意一个正在播放的视频，滑动速度条，最大速度为 7，点击上述功能键（移动方向、调焦控制、聚焦控制、光圈控制），相机会以选中的速度执行选中的功能。
	光圈控制 光圈-/光圈+	缩小/放大光圈，通过调节镜头的光线来调整监控画面的亮度。
	灯光	打开或关闭灯光。

	雨刷	单击“雨刷”按钮 ，雨刷可以清除镜头上的东西，使得画面变得清晰。
	辅助聚焦	单击辅助聚焦按钮，自动完成聚焦动作。
	镜头初始化	在调焦后图像仍然模糊的情况下，单击镜头初始化按钮，镜头自动重新校准并聚焦，使得图像变得清晰。
	菜单	打开设备主菜单，执行相关操作。
	开启手动跟踪	当开启跟踪功能时单击 按钮并选中需要跟踪的目标，就可对该目标进行跟踪。
	开启 3D 定位	根据用户选择的点位或区域自动调整云台的位置和焦距。 单击后，按住鼠标左键在画面中单击某个点或框选所关注的区域，进行自动放大/缩小。方便用户查看所关注区域的画面细节。

7.2.2 设置预置点、巡航路径

云台控制支持设置和调用预置点、巡航路径。

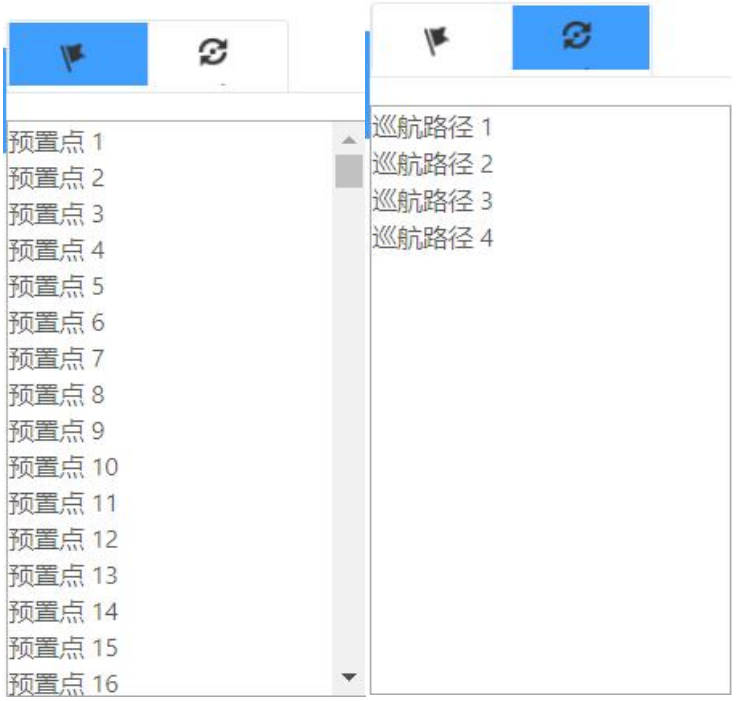


图 7-3 预置点/巡航路径

说明

预置点操作步骤

除特殊预置点外，其他预置点均可以用来保存云台的位置信息，以便以后调用该预置点方位。

步骤 1：单击“ ”，将出现预置点操作界面，操作云台控制的方向键，使云台转到需要保存的方位。

步骤 2：单击除特殊预置点的其他点位行，双击预置点名称处即可修改预置点名称。

步骤 3：单击“ ”可调用该预置点，单击“ ”，可清除该预置点的信息。

巡航扫描操作步骤

巡航扫描是指根据设定的预置点进行自动扫描。

步骤 1：单击“ ”转到“巡航路径”设置界面，选择需要设置的巡航路

径。

步骤 2：单击“ ”可设置巡航点，可添加巡航所设置的预置点；请以相同方式设置其他巡航点。

单击“ ”可开启巡航扫描，单击“ ”可停止巡航扫描，单击“ ”可删除巡航扫描。

任务	功能	操作说明
预置点	某个预定义的图像位置，当需要快速监控某个目标时，可通过控制设备的调用命令调出预先设置好的监控点。	设置：
		调用：
巡航路径	在云台固定几个预置点之间来回运动的状态，并可设置两个预置点之间的巡航时间。注：设置巡航前，需添加至少两个预置点。	

8. 录像回放

视频回放可回放接入前端摄像机的视频。回放页面支持视频倒放、慢放、快放、视频停止播放、视频暂停。回放支持视频全部停止回放、解密回放、视频验签、视频截图、视频剪辑和全屏预览，支持抓图和录像下载功能。

图标	名称	功能说明
	倒放	从后面开始播放，逆放。
	单帧	点击“单帧”则会变成下一帧，再次点击“播放”键，就会继续使用播放功能。

	/快放/慢放	点击“快放/慢放”会快速/缓慢播放，在这个过程中点击“播放”则会暂停。
	停止	在视频回放播放中，点击“停止“按钮，视频回放结束。
	播放	在中心存储 CVR 列表中选择要查看回放的设备，点击“播放”按钮（可以指定回放视频的日期时间），相机播放选中日期的视频，点击“暂停”按钮，视频回放暂停。

8.1 回放工具栏

图标	名称	功能说明
	全部停止回放	回放全部停止播放。
	解密	————————————
	验签	————————————
	抓图	可对需要保存的画面进行手动抓图。
	开始剪辑	点击“剪辑”按钮，可以对回放视频进行编辑。
	启用电子放大	点击“电子放大”按钮，光标移至预览窗口上并滚动滚轮，可放大播放画面。
	下载	在视频播放前点击下载按钮，结束后再次点击，回放录像被

		下载。
	全屏	全屏显示视频播放界面。

说明

回放日期：可查看当天视频，也可选择固定日期固定时间，需手动选择。如图 8-1 所示。

图 8-1 日期选择

8.2 视频验签

进入视频回放页面，即可对历史视频做签名验签操作，右下方红框中是显示历史视频的验签状态以及签名值，点击验签按钮后即可对存储的视频进行验签。如图 8-2 所示。

图 8-2 视频验签

9. 日志

9.1 日志查询

单击“日志”进入日志界面，日志界面可以查询、显示、导出日志信息。可查询接入的视频安全转换器设备报警信息：设备掉线、设备上线、设备注册异常、视频验签失败等报警日志。设备界面如图 9-1 所示。

图 9-1 日志

说明

您可以选择日志的主类型和次类型以及查询的时间，单击“查找”，列表中将显示符合条件的日志信息。

单击“导出”，可以将日志信息保存至本地计算机。

9.2 诊断信息

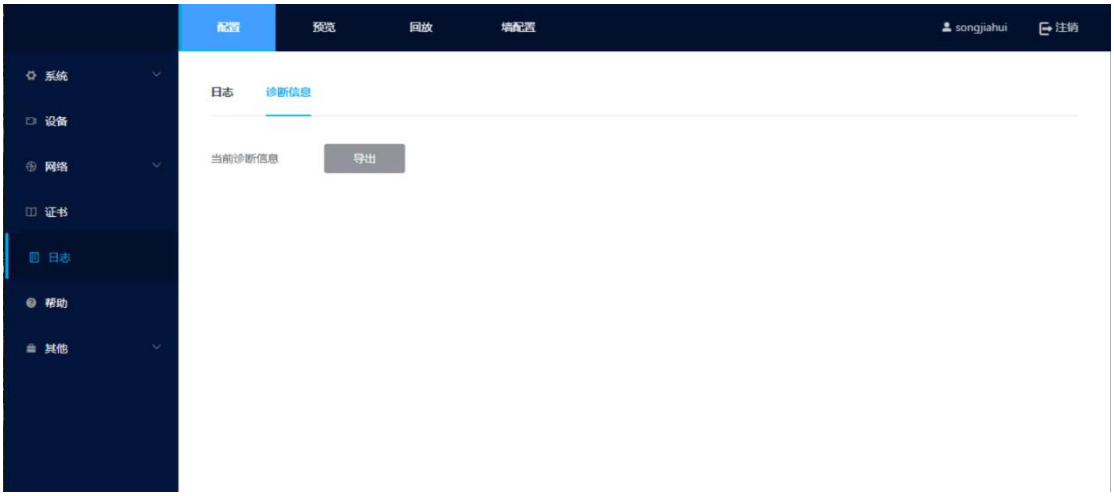


图 9-2 诊断信息

10.ONVIF 设备

可将视频安全服务系统接入的视频以 ONVIF 协议接入其他服务平台。ONVIF 设备列表需配置 IP 地址、管理端口、视频通道编码 ID。注：视频通道编码 ID 必须在视频服务系统中存在。如图 10-1 所示。

图 10-1 ONVIF 设备

10.1 批量添加

可在线添加 ONVIF 设备。单击“批量添加”，进入批量添加界面。可批量添加 ONVIF 设备关联通道数据。如图 10-2 所示。

单击“添加”，新增一行，输入 IP 地址、管理端口、用户名、密码，视频通道编码 ID（选择可用视频通道）可添加一条或多条数据。

选择某一行，单击“删除”，删除 ONVIF 配置数据。

添加完成后，单击“确定”，保存录入数据，录入的数据显示在 ONVIF 设备界面列表中。

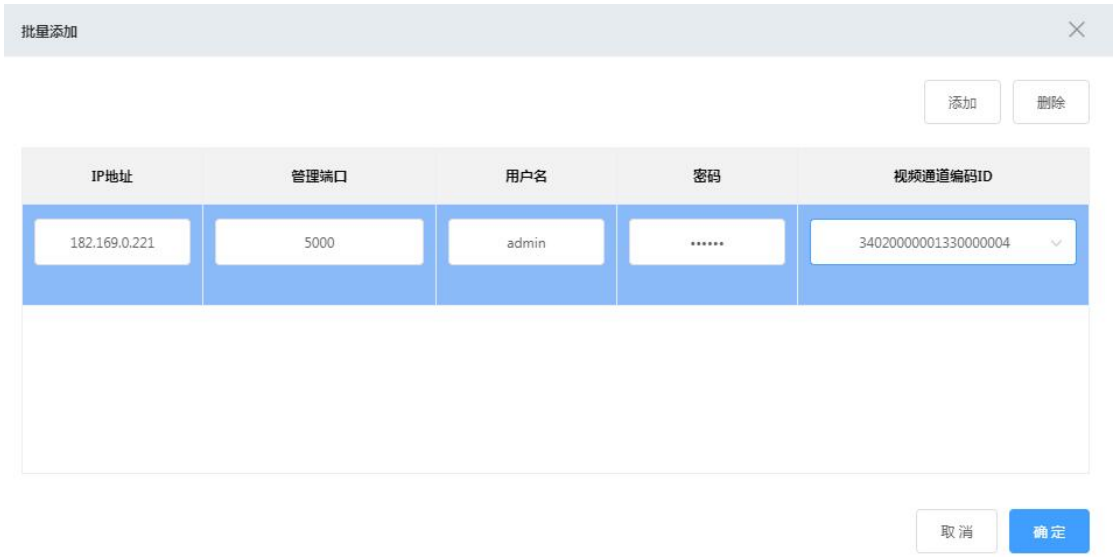


图 10-2 批量添加

10.2 下载模板

可离线导入配置的 ONVIF 设备。

单击“下载模板”按钮，将 ONVIF 设备导入模板下载到本地计算机。如图 10-3 所示。

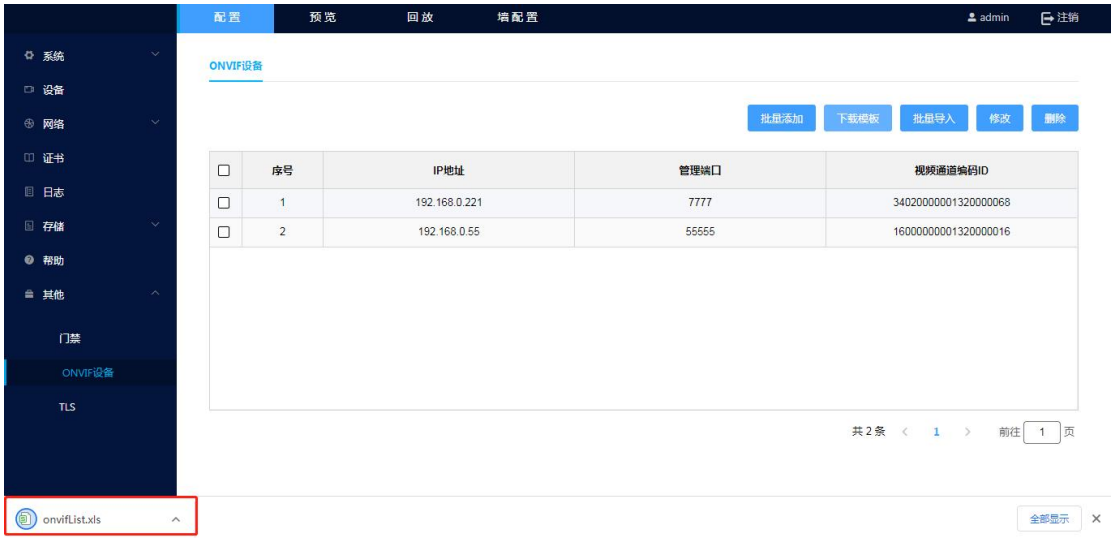


图 10-3 下载模板

注意

模板如图 12-4 所示。根据注意事项维护数据，完成后保存。

注意事项：
1. IP地址和管理端口组合不能重复。
2. 视频通道编码ID需在视频安全服务系统中存在。
3. 所有字段不能为空。

IP地址	管理端口	用户名	密码	视频通道编码ID

图 10-4　ONVIF 模板数据

10.3 批量导入

单击“批量导入”，选择文件可将模板中数据导入到 ONVIF 设备数据列表中。数据维护正确时，ONVIF 设备列表自动展示导入的数据。如图 10-5 所示。

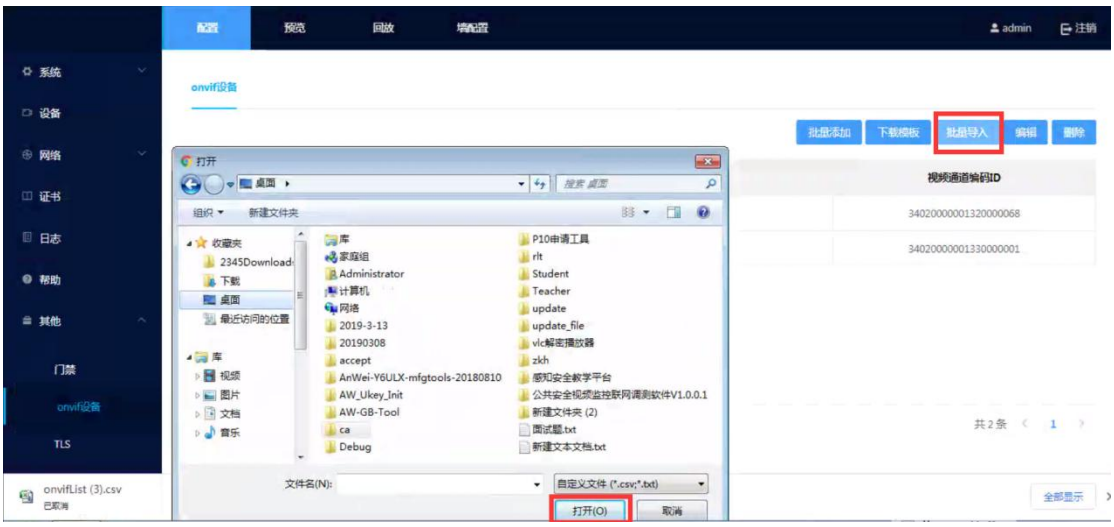


图 10-5 批量导入

导入的数据有误时，导入时返回添加失败的数据，可根据行号和对应的错误详情修改数据，修改正确后再次导入。如图 10-6 所示。

图 10-6 添加失败数据

10.4 修改

选择要修改的数据，单击“修改”按钮，可修改列表信息。如图 10-7 所示。

图 10-7 ONVIF 设备修改

10.5 删除

选择要删除的数据，单击“删除”按钮，弹出提示信息“此操作将删除数据，是否继续？”，单击“确定”按钮，数据从列表清除。可一次删除多条数据。如图 10-8 所示。

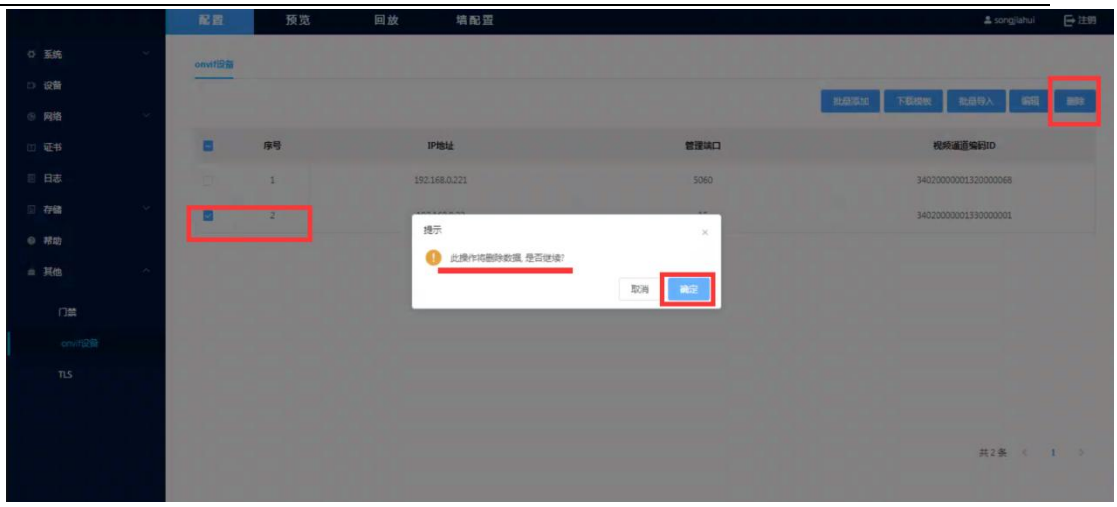


图 10-8 ONVIF 设备删除

11.TLS

TLS 用于在两个通信程序之间提供保密性和数据完整性，通过 TLS 可先将数据进行加密再进行传输。

门禁一体机接入视频安全转换器，视频安全转换器与视频安全服务平台建立国密 TLS 加密安全通道，门禁一体机通过加密通道进行应用数据的安全传输；视频安全服务平台通过门禁管理平台订阅刷卡门禁事件，视频安全服务平台将订阅的刷卡门禁事件进行备份存储，并采用 SM2 算法对备份数据进行签名，视频安全服务平台提供门禁刷卡日志记录的验签功能，以提供验证门禁刷卡记录的合法性功能。

TLS 加密通道有两种模式：TLS 客户端、TLS 服务端。如图 11-1 所示。

图 11-1 TLS 加密界面

11.1 TLS 客户端

选择“其他→TLS→TLS 客户端”，TLS 客户端模式界面包括信息有客户端 IP、客户端管理端口、服务端 IP、服务端管理端口、证书状态、是否启用等信息。如图 11-2 所示。

图 11-2 TLS 客户端

11.1.1 批量添加

选择“TLS 客户端→批量添加”，进入 TLS 客户端批量添加界面，单击“添加”按钮，可添加一条数据，添加完成后可再次单击添加数据。选中添加的数据行，单击“删除”可删除添加的数据。如图 11-3 所示。

图 11-3 TLS 客户端批量添加

11.1.2 删除

勾选要删除的数据，单击“删除”按钮，提示“此数据将删除该条数据，是

否继续？”点击“确定”，TLS 客户端数据列表没有此条数据。如图 11-4 所示。

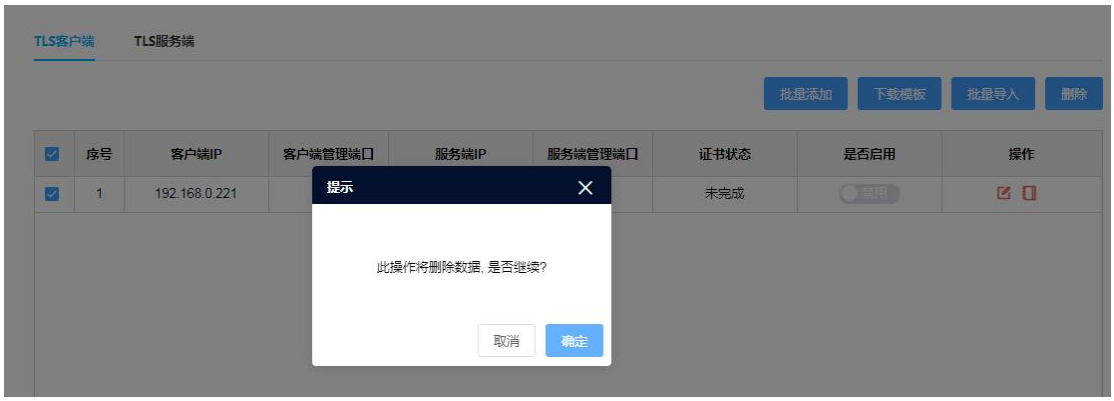


图 11-4 删除 TLS 客户端数据

11.1.3 下载模板

单击“下载模板”按钮，可将批量维护 TLS 客户端数据的模板下载至本地计算机。如图 11-5 所示。

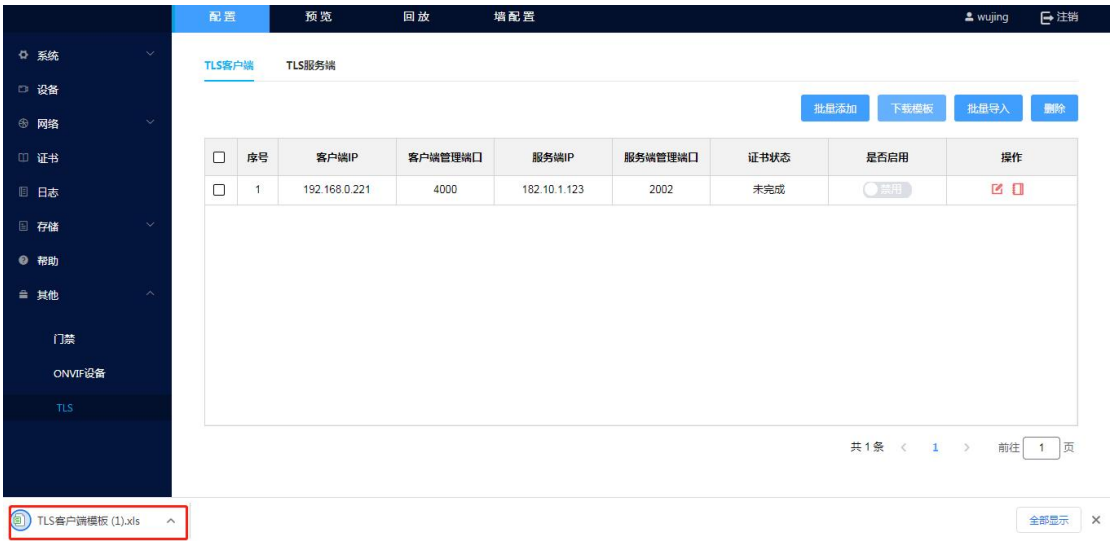


图 11-5 下载模板

注意

模板数据如图 11-6 所示。数据维护时需注意：

（1）IP 地址和管理端口组合不能重复。

（2）所有字段不能为空。

注意事项：
1. IP地址与端口号组合不能重复
2. 所填项不能为空

客户端IP地址	客户端端口号	服务端IP地址	服务端端口号

图 11-6 TLS 客户端批量维护数据模板

11.1.4 批量导入

在 TLS 客户端批量导入模板中维护好数据，保存。单击“批量导入”，选择要导入的数据文件，导入后，提示“导入成功”。界面如图 11-7 所示。

图 11-7 TLS 客户端批量导入

导入时检验数据正确性，可根据添加失败数据界面的行号和错误详情修改数据，修改正确后导入。如图 11-8 所示。

图 11-8 TLS 客户端批量导入失败数据

11.1.5 TLS 客户端修改

单击 TLS 客户端行项目中操作列的“修改”：可更改服务端 IP、服务端管理端口、客户端 IP、客户端管理端口。如图 11-9 所示。

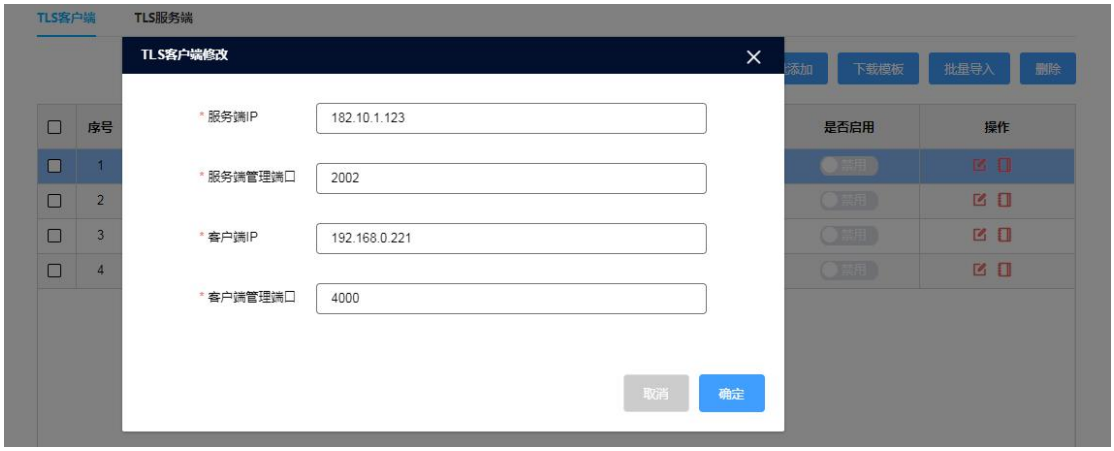


图 11-9 TLS 客户端修改

11.1.6 TLS 客户端证书导入

单击 TLS 客户端行项目中操作列的“证书导入”，导入安装证书。如图 11-10 所示。

图 11-10 TLS 客户端证书导入

11.2 TLS 服务端

选择“其他→TLS→TLS 客户端”，TLS 客户端模式界面包括信息有服务端 IP、服务端管理端口、证书状态、是否启用等信息。如图 11-11 所示。

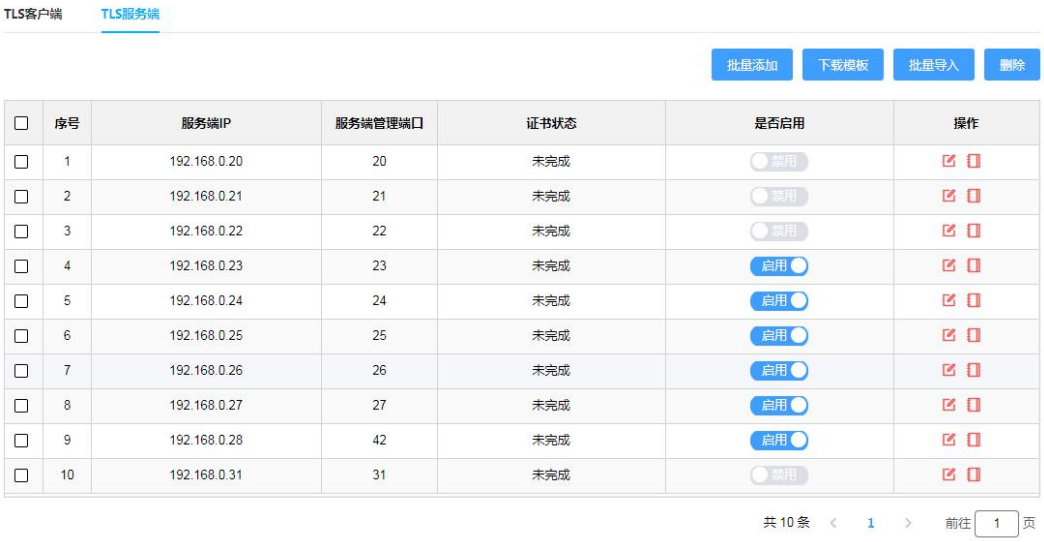


图 11-11 TLS 服务端

11.2.1 批量添加

选择“TLS 服务端→批量添加”，进入 TLS 服务端批量添加界面，单击“添加”按钮，可添加一条数据，添加完成后可再次单击添加数据。选中添加的数据行，单击“删除”可删除添加的数据。如图 11-12 所示。

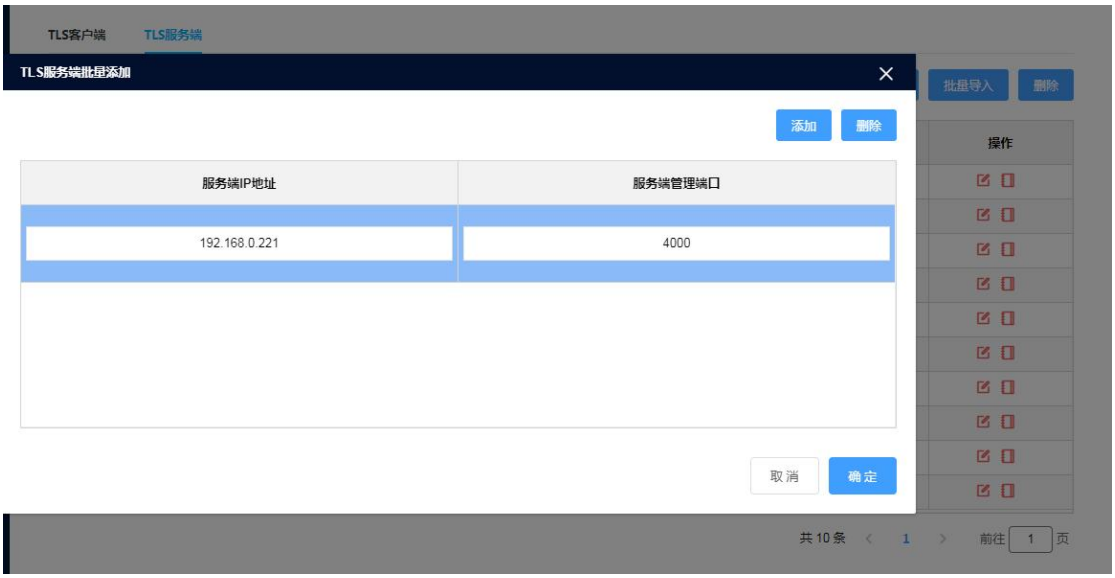


图 11-12 TLS 服务端批量添加

11.2.2 删除

勾选要删除的数据，单击“删除”按钮，提示“此数据将删除该条数据，是否继续？”点击“确定”，TLS 服务端数据列表没有此条数据。如图 11-13 所示。

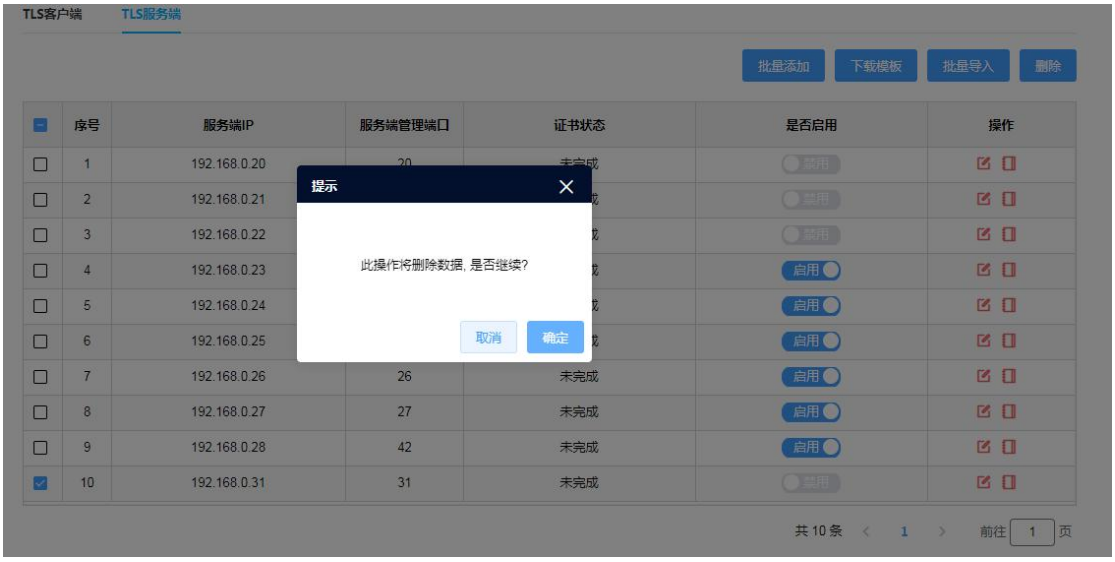


图 11-13 删除 TLS 服务端数据

11.2.3 下载模板

单击“下载模板”按钮，可将批量维护 TLS 服务端数据的模板下载至本地计算机。如图 11-14 所示。

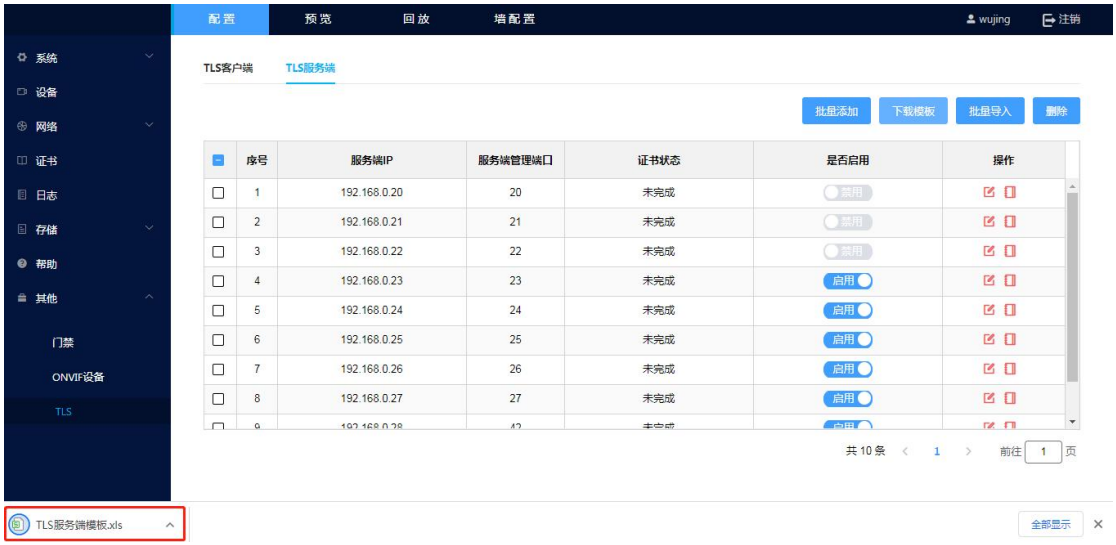


图 11-14 下载模板

注意

模板数据如图 11-15 所示。数据维护时需注意：

（1）IP 地址和管理端口组合不能重复。

（2）所有字段不能为空。

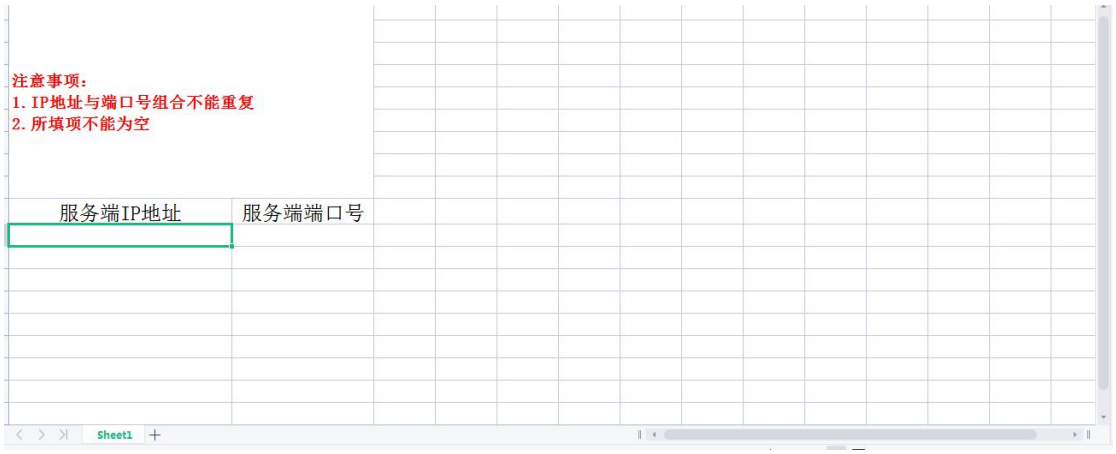


图 11-15 TLS 服务端批量维护数据模板

11.2.4 TLS 服务端批量导入

在 TLS 服务端批量导入模板中维护好数据，保存。单击“批量导入”，选择要导入的数据文件，导入后，提示“导入成功”。界面如图 11-16 所示。

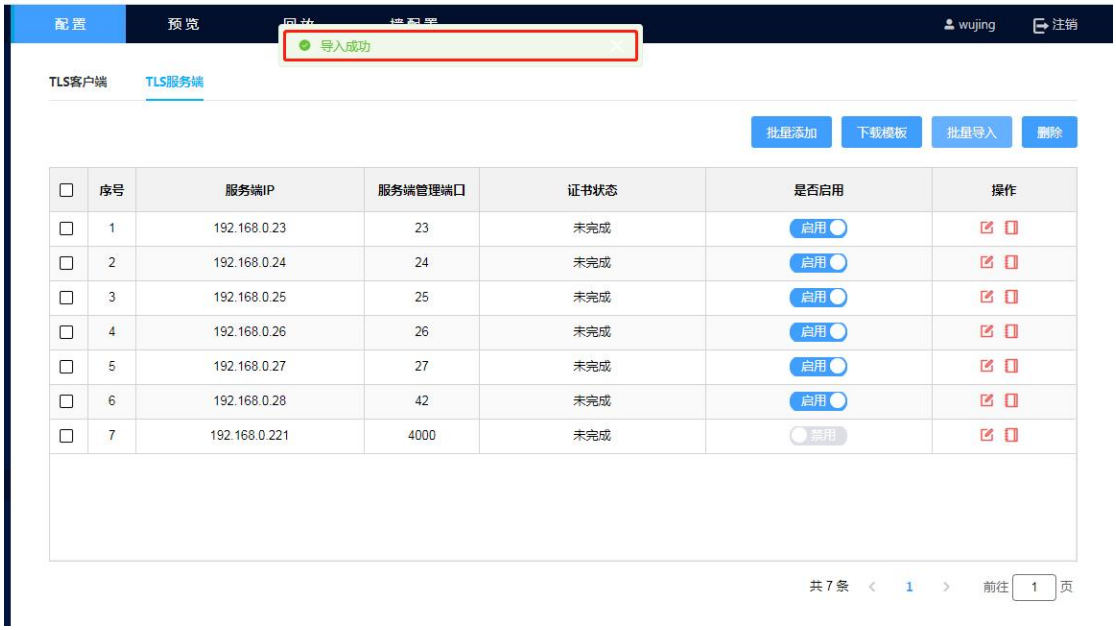


图 11-16 TLS 服务端批量导入

导入时检验数据正确性，可根据添加失败数据界面的行号和错误详情修改数据，修改正确后导入。如图 11-17 所示。

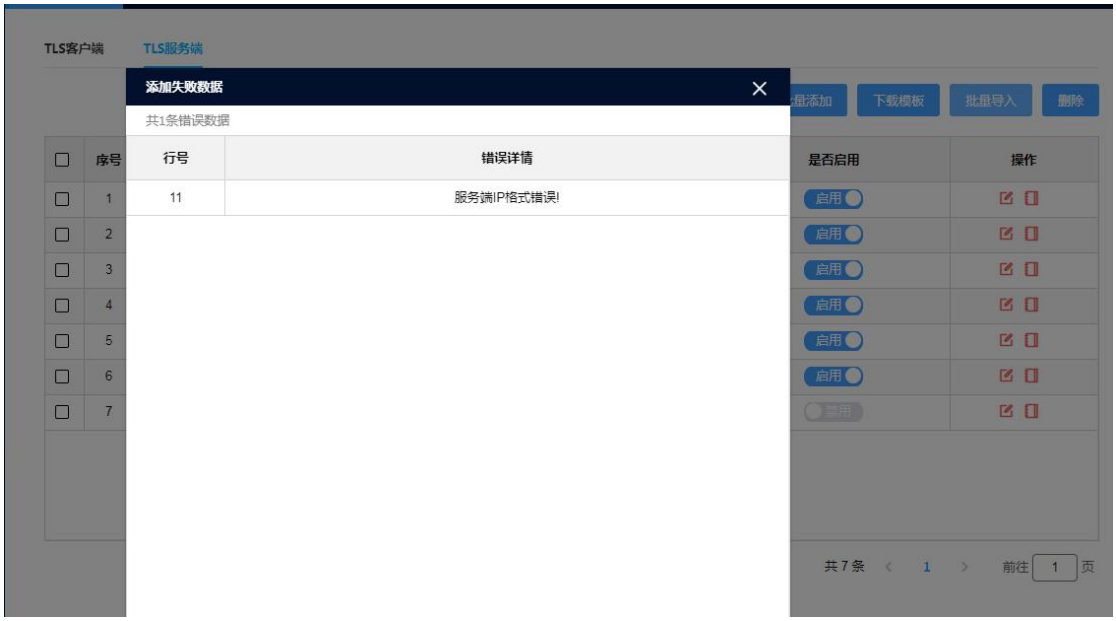


图 11-17 TLS 服务端批量导入失败数据

11.2.5 TLS 服务端修改

单击 TLS 服务端行项目中操作列的“修改”：可更改服务端 IP、服务端管理端口。如图 11-18 所示。

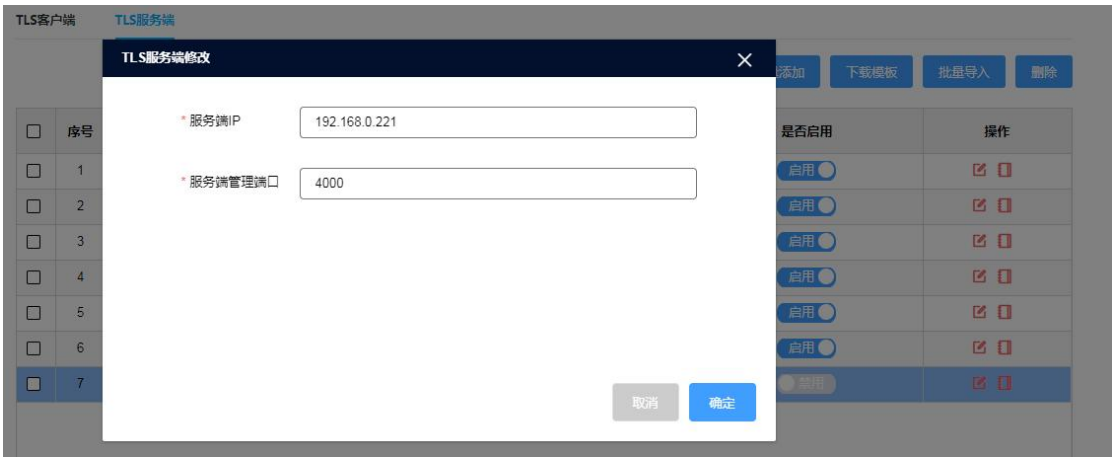


图 11-18 TLS 服务端修改

11.2.6 TLS 服务端证书导入

单击 TLS 服务端行项目中操作列的“证书导入”，导入安装证书。如图 11-19 所示。

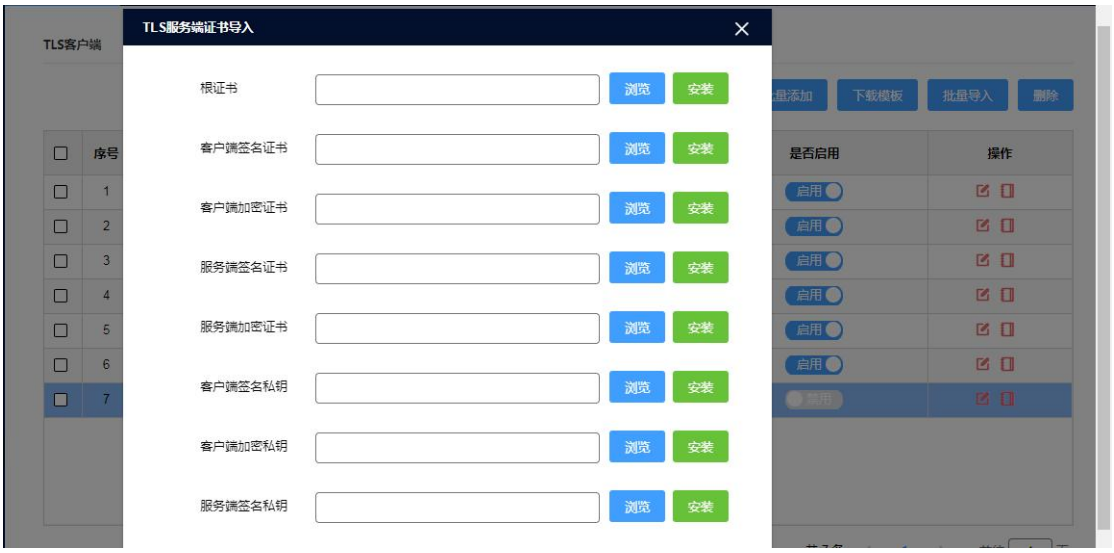


图 11-19 TLS 服务端证书导入

12.门禁

点击“门禁”，进入门禁验签的页面，门禁数据是从门禁系统读取到的数据并且已经存入视频安全服务系统的数据库中，并且对任意一条数据进行签名验签的操作。点击验签按钮，即可对门禁数据进行完整性校验。如图 12-1 所所示。

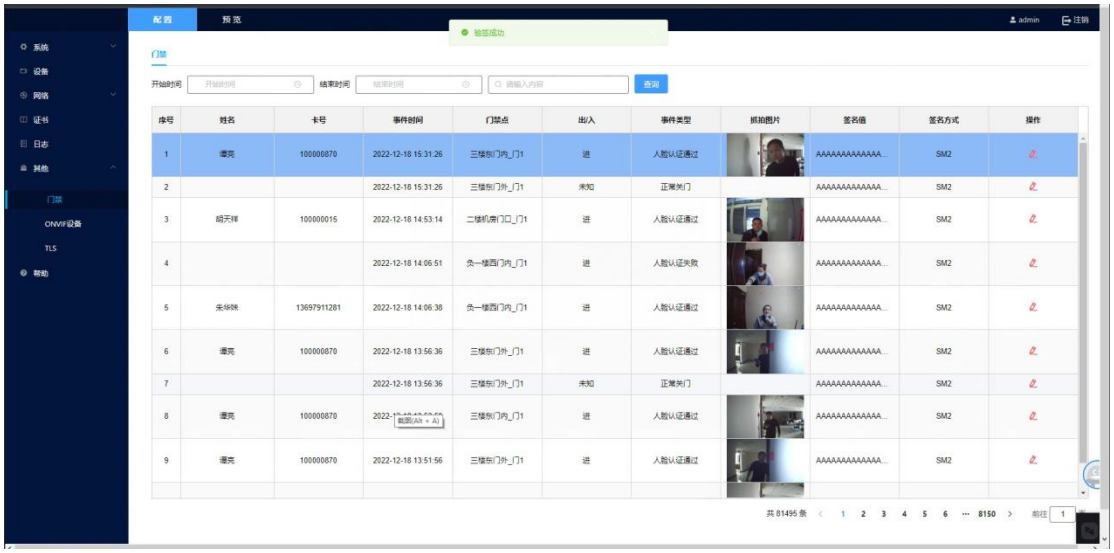


图 12-1 门禁验签