



安为科技
Anwei Tech

四路视频安全转换器
（GB 34115 C 级）
操作手册

法律声明

版权所有©北京安为科技有限公司。保留一切权利。

本手册的任何部分，包括文字、图片、图形等归属于北京安为科技有限公司（以下简称“本公司”或“安为科技”）。未经书面许可，任何单位和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。

关于本手册

本手册描述的产品仅供中国大陆地区销售和使用。

本手册作为指导使用。手册中所提供的照片、图形、图标和插图等，仅用于解释和说明目的，与具体产品可能存在差异，请以实物为准。因产品版本升级或其他需要，本公司可对本手册进行更新，如您需要最新版手册，请您登录公司官网查阅。（<http://www.anweitech.com>）。

安为科技建议您在专业人员指导下使用本手册。

商标声明



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，本手册所描述的产品（含其硬件、软件等）均“按照现状”提供，可能存在瑕疵、错误、或故障，本公司不提供任何形式的明示或默认保证。亦不对使用本手册或使用本公司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、数据或文档丢失产生的损失。
- 若您将产品接入互联网需自担风险，包括但不限于产品可能遭受网络攻击、黑客攻击、病毒感染等，本公司不对因此造成的产品工作异常、信息泄露等问题承担责任，但本公司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。若本产品被用于侵犯第三方权利或其他不当用途，本公司概不承担任何责任。
- 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

本手册适用于安为视频安全转换器产品：AWS-Model-210。

本节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	说明类文字，表示对正文的补充和解释。
 注意	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	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



- 视频安全加固模组的安装施工须符合规范，可参照相关国家标准或地方标准。
- 若将视频安全加固模组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。
- 视频安全加固模组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，并将视频安全加固模组安装在儿童、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。



- 若视频安全加固模组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）。
- 请定期对视频安全加固模组进行保养与维护，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，请你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加固模组的全部原包装材料，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。

目录

- 1.产品简介 7
 - 1.1 产品说明 7
 - 1.2 产品功能 7
 - 1.3 产品特性 8
 - 1.4 产品参数 8
 - 1.5 产品外观 9
- 2.操作须知 10
 - 2.1 系统登录与退出 10
 - 2.2 主界面说明 11
- 3.系统参数设置 12
 - 3.1 系统设置 12
 - 3.1.1 基本信息 12
 - 3.1.2 时间配置 12
 - 3.1.3 升级维护 13
 - 3.1.4 日志 14
 - 3.1.5 关于设备 15
- 4.网络参数设置 16
 - 4.1 基本配置 16
 - 4.2 高级配置 16
 - 4.2.1 平台接入 17
 - 4.2.228181 服务 18
 - 4.2.3 证书管理 19
 - 4.2.4TLS 20
- 5.安全管理 22
- 6.用户管理 23
 - 6.1 用户添加 24
 - 6.2 用户修改 25
 - 6.3 用户删除 25

- 7.通道管理 26
 - 7.1 设备添加 26
 - 7.2 设备修改 28
 - 7.3 设备删除 28
- 8.录像预览 29
 - 8.1 预览工具栏 29
 - 8.2 云台控制 30
 - 8.2.1 云台控制面板 30
 - 8.2.2 设置预置点、巡航路径 32

1. 产品简介

1.1 产品说明

AWS-Model-210C 四路视频安全转换器是一款面向已建视频监控系统，实施“利旧”性安全改造的产品;转换器设备内置国产商用密码芯片，支持 SM1、SM2、SM3、SM4 算法，支持数字证书和密钥的安全存储，满足 GB 35114 C 级要求，支持双向身份认证，支持控制信令的完整性保护;可以为已装网络摄像机提供便利的设备身份认证、控制指令完整性校验、H.264、H.265 编码转换 SVAC 2.0 编码、视频流加密、视频关键帧签名、内外网隔离、协议白名单等安全功能。

本产品可广泛应用于军队、保密、公安等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网络摄像机设备提供便利的安全加固，快速实现对标 GB 35114-2017 C 级的设备安全性提升。

1.2 产品功能

支持商用密码算法 SM1~SM4

WEB 配置、安全登录、白名单配置、日志管理

支持 4 路网络摄像机接入，支持 GB/T 28181、GB 35114、ONVIF 等多种视频接入协议，支持 GB/T 28181ONVIF 与 GB 35114 互转

支持符合 GB35114-2017 标准要求的双向设备身份认证，认证时延小于 400ms，支持使用 SM3 算法按照 GB 35114 标准规定的方式实现控制信令的完整性校验

支持并发 4 路 H.264/H.265 码流转换为 SVAC 码流，并采用 GB 35114 B 级方式实现对码流关键帧的完整性保护

支持基于 SM1-OFB 模式和 SM4-OFB 模式采用 GB 35114 C 级方式实现对码流的加密防护，视频加解密增加时延不超过 400ms

支持基于数字证书的用户认证、支持单向双向设备身份认证，支持控制信令认证

支持基于 SM2 算法音视频流签名

支持基于 SM1、SM4 算法音视频流加密

支持在视频数据帧层面添加自定义标识支持日志管理，提供操作日志、报警日志、异常日志的纪录和查询。

1.3 产品特性

本产品采用“五网口”设计，内置商用密码算法芯片，可以实现网络摄像机与后台系统的逻辑隔离。本产品对照 GB 35114-2017 C 级防护要求，可在 SIP 信令层面实现基于 SM2 数字证书的身份认证和控制指令安全防护，以及对 H.264/H.265 编码格式的视频流进行数字签名和加密的安全防护，在不需要改动前端视频设备的条件下，实现前端设备的安全性增强。本产品可实现四路视频终端设备的安全加固，即 4 个对内网口连接四个终端设备，一个对外网口连入系统交换设备。

1.4 产品参数

规格/型号		AWS-Model-210C
视频	接入压缩标准	H.264、H.265
	输出压缩标准	SVAC2.0
	支持视频路数	四路
	H.265 编码类型	Main Profile
	H.264 编码类型	Main Profile/High Profile
功能	音频编码	G711U/G711A
	网络对时	支持
	IP 自适应	支持
	远程操作	视频播放、系统管理、网络管理、证书管理、用户管理
	国标 35114	支持
	国标 28181	支持

	视频安全	SVAC2.0 视频签名、视频加密
网络	以太网	5 个 RJ-45 接口，10M/100M 自适应
	网络协议	标准 HTTP,TCP/IP,ICMP.RTSP,RTP,UDP,RTCP,SMTP,DHCP,DNS
	接入协议	标配 ONVIF、RTSP、GB/T 28181
	输出协议	GB 35114-2017
	浏览器	支持 IE8+,Chrome18+,Firefox5.0+,Safari5.02+浏览器、支持中文
	用户权限	最多 10 个用户，分 2 级权限：管理员、普通用户
一般 规范	电源	DC12V 2A
	尺寸	210mm*160mm*30mm
	工作温度	-30℃~+60℃
	工作湿度	10%~90%
	功率	<5W
	颜色/材质	黑色/铝合金

1.5 产品外观



序号	名称	功能说明
1	电源接口	接入 DC52V 电源
2	电源指示灯	设备通电时常亮
3	一个 WAN 网络接口	接入后端网络设备
4	4 个 LAN 网络接口	接入前端视频设备

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和视频安全转换器，您可在浏览器中输入视频安全转换器的 IP 地址 <https://192.168.0.XX> 登录。首次登录视频安全加固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（非管理员用户）需联系管理员重置密码。



图 2-1 登录界面

退出系统

当进入视频安全加固系统主界面时，您可点击右上角的“ [注销]”安全退出系统。

2.2 主界面说明

在视频安全加固系统主界面上，您可以进行视频预览和配置系统功能，界面如图 2-2 所示。

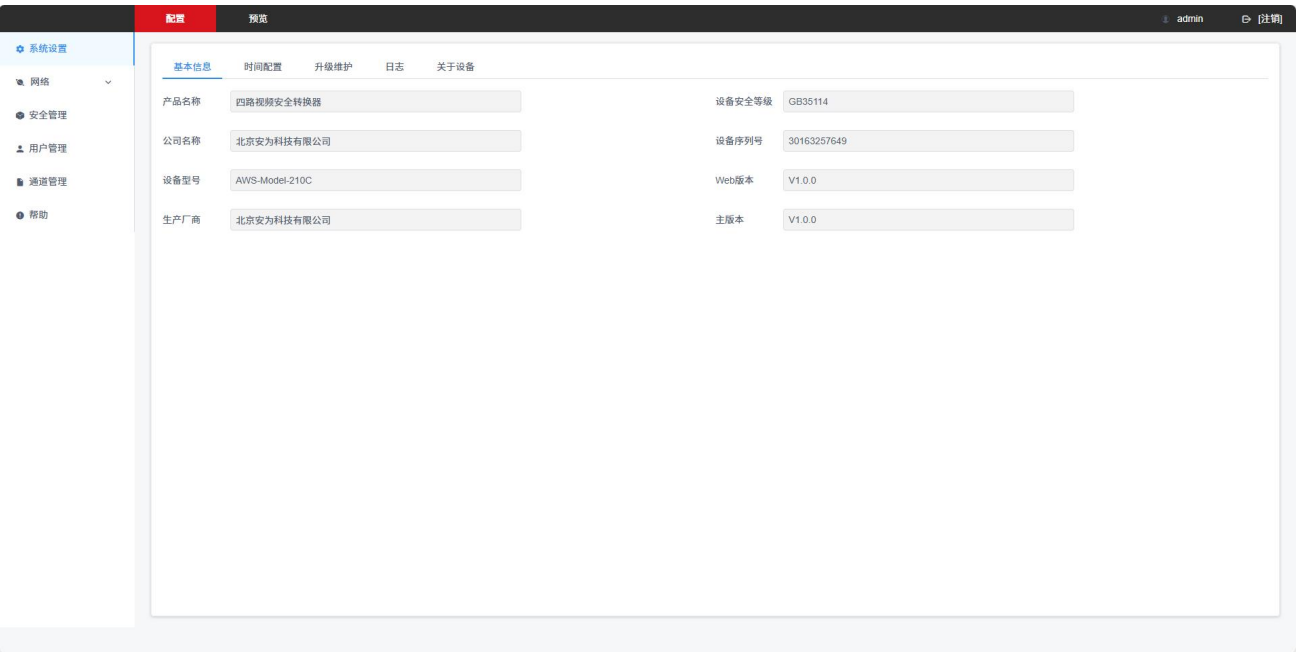


图 2-2 主页面



预览：用户网络摄像机监控画面预览及参数调节。

配置：进入视频安全转换器配置界面进行系统配置及功能配置。

3. 系统参数设置

3.1 系统设置

选择“配置→系统设置”，系统设置包括基本信息、时间配置、升级维护、日志、关于设备等参数。

3.1.1 基本信息

选择“配置→系统设置”，单击“基本信息”页面，可查看视频安全转换器的系统信息。

视频安全转换器基本信息包括产品名称、设备安全等级、公司名称、设备序列号、设备型号、软件版本号、生产厂商、主版本信息，上述信息均从设备中读取，无法手动修改，界面如图 3-1 所示。

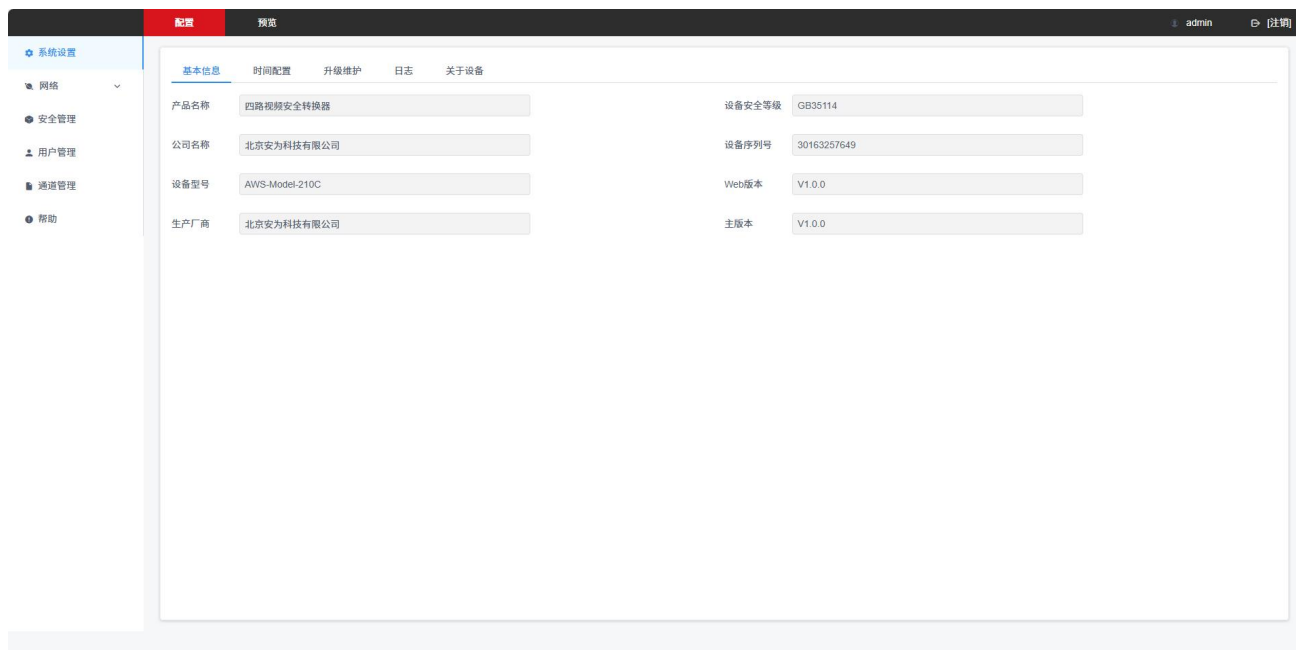


图 3-1 基本信息

3.1.2 时间配置

选择“配置→系统设置”，单击“时间配置”页面可对视频安全转换器时区进行校时，界面如图 3-2 所示。

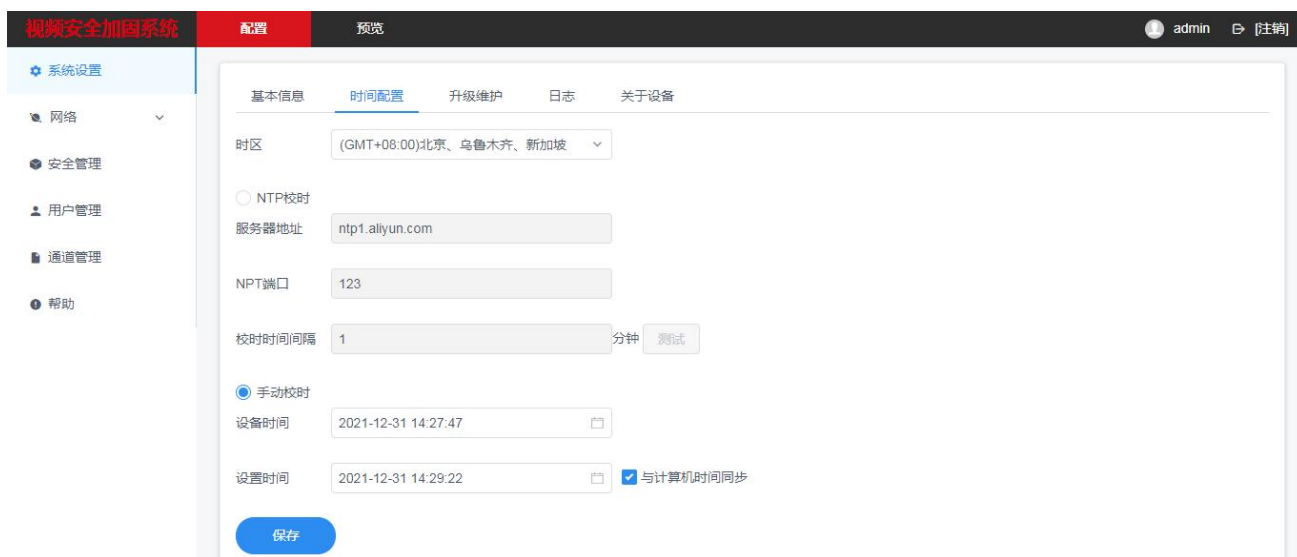


图 3-2 时间设置



设备时区：进入时间配置界面，可以对视频安全转换器进行校时。“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”检测视频安全转换器与 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。

3.1.3 升级维护

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



图 3-3 升级维护



说明

单击“重启”按钮，可重启前端设备。系统弹出“是否重启设备”，单击“确定”按钮，系统重启。

单击“恢复出厂设置”，恢复设备参数到出厂设置默认值。

单击“浏览”按钮，选择升级文件，单击“升级”按钮，如文件错误，提示“设备升级失败，请稍后重试！”，如文件正确，提示“系统升级成功后设备将自动重启，确定升级？”，单击确定，系统升级中，升级完成系统跳转至登录页面。

3.1.4 日志

选择“配置→系统设置”，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。界面如图 3-4 所示。

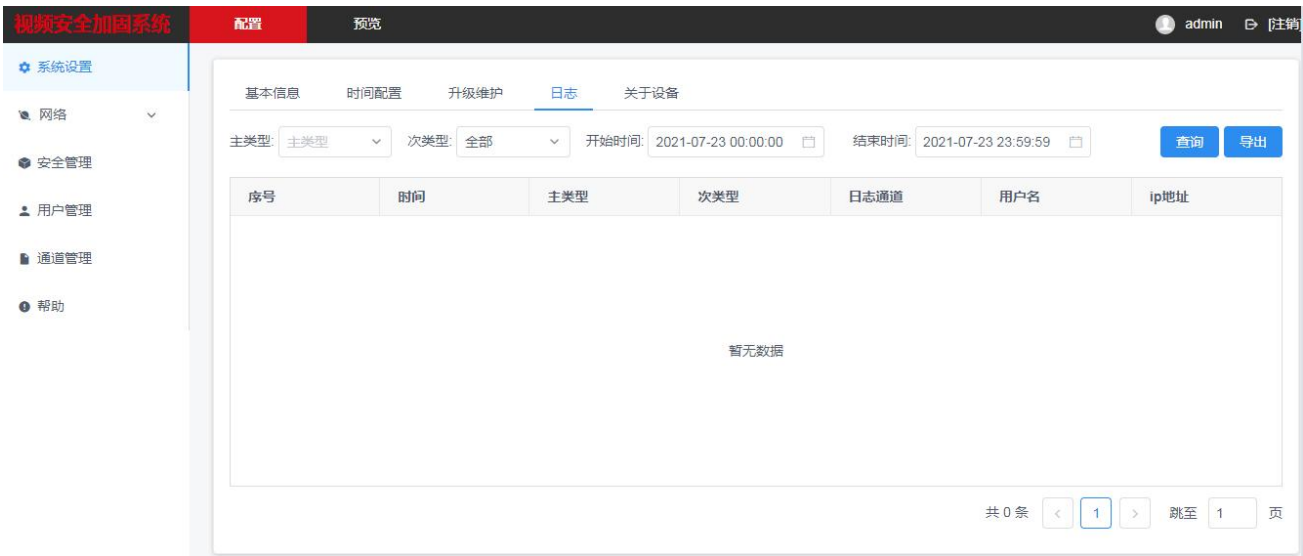


图 3-4 日志



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。

3.1.5 关于设备

选择“配置→系统设置”，单击“关于设备”进入关于设备界面，主要对视频设备安全加固盒产品进行详细说明。如图 3-5 所示。



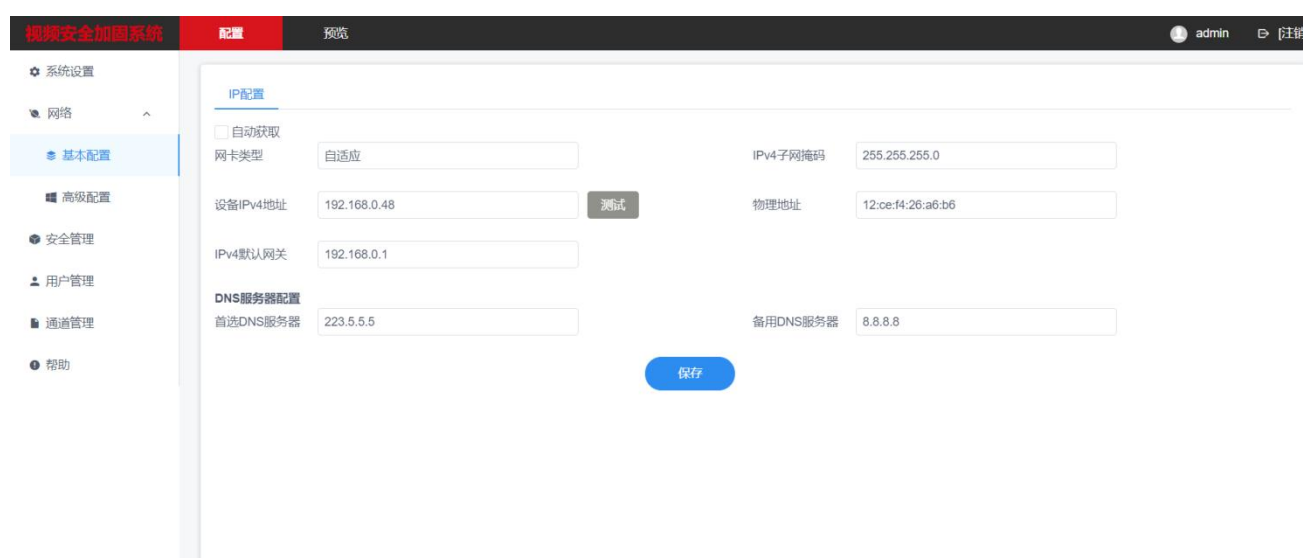
图 3-5 关于设备

4. 网络参数设置

选择“配置→网络”页面将显示基本配置和高级配置。

4.1 基本配置

选择“配置→网络→基本配置”进入“基本配置”页面。主要配置内容：网卡类型、IPv4 子网掩码、设备 IPv4 地址、物理地址、IPv4 默认网关、首选 DNS 服务器、备用 DNS 服务器，如图 4-1 所示。



The screenshot shows the 'Basic Configuration' page of the AWS-Model-210C network management system. The page is titled 'IP配置' (IP Configuration). It contains the following fields and options:

- ☐ 自动获取 (Automatic Acquisition)
- 网卡类型 (Network Card Type): 自适应 (Adaptive)
- 设备IPv4地址 (Device IPv4 Address): 192.168.0.48
- IPv4子网掩码 (IPv4 Subnet Mask): 255.255.255.0
- 物理地址 (Physical Address): 12:ce:f4:26:a6:b6
- IPv4默认网关 (IPv4 Default Gateway): 192.168.0.1
- DNS服务器配置 (DNS Server Configuration)
- 首选DNS服务器 (Preferred DNS Server): 223.5.5.5
- 备用DNS服务器 (Backup DNS Server): 8.8.8.8

A '测试' (Test) button is located next to the device IPv4 address field. A '保存' (Save) button is located at the bottom center of the configuration area.

图 4-1 基本配置



说明

在 IP 配置界面，通过勾选“自动获取”，系统能够自动获取设备 IP 地址；您也可以手动输入相关的网络参数，单击“测试”，可检测该 IP 地址是否被占用。

DNS 服务器配置正确的可用的服务器地址后，需要域名访问的功能才可正常使用。

参数配置完成后单击“保存”完成参数配置。

4.2 高级配置

选择“配置→网络→高级配置”进入“高级配置”页面。高级配置界面包括“平台接入”、“28181 服务”。



说明

视频设备安全加固终端支持 GB/T28181 和 GB35114 两种协议的转换。安全加固终端融合

国密安全芯片支持 GB35114 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/T28181 向 GB35114 的协议转换，并连入上级 35114 视频安全管理平台。

4.2.1 平台接入

选择“配置→网络→高级配置→平台接入”，配置平台接入页面参数，勾选“启用”，即可实现平台接入，如图 4-2 所示。

图 4-2 平台接入



平台接入界面配置参数说明：

- 平台接入方式为 GB35114-2017，不可修改。
- 本地 SIP 端口：本级安全加固终端向上级 35114 视频安全管理平台进行 SIP 信令通信的端口号，默认 5060，范围 1025-65535。
- SIP 服务器 ID：注册到上级 35114 视频安全管理平台的目的 SIP 服务器 ID，20 位数字。
- SIP 服务器域：公安平台的 SIP 域编号，为 SIP 服务器 ID 的前 10 位。
- SIP 服务器地址：注册到上级 35114 视频安全管理平台的目的 SIP 服务器 IP 地址。
- SIP 服务器端口：注册到上级 35114 视频安全管理平台的 SIP 服务器 35114 服务端口号，默认为“5060”，范围 1025-65535。
- SIP 用户认证 ID：本级安全加固终端的 SIP 服务器编号，设备唯一标识。
- 注册有效期：安全加固终端注册到上级 35114 视频安全管理平台的有效期限。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。
- 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。

- 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上级 35114 视频安全管理平台连接。系统默认最大超时次数为 3 次，建议采用默认值，范围 3-255。

参数配置完成后单击“保存”完成参数配置。

4.2.228181 服务

选择“配置→网络→高级配置→28181 服务”输入 28181 服务参数，勾选“启用”，即可实现 28181 服务接入，如图 4-3 所示。

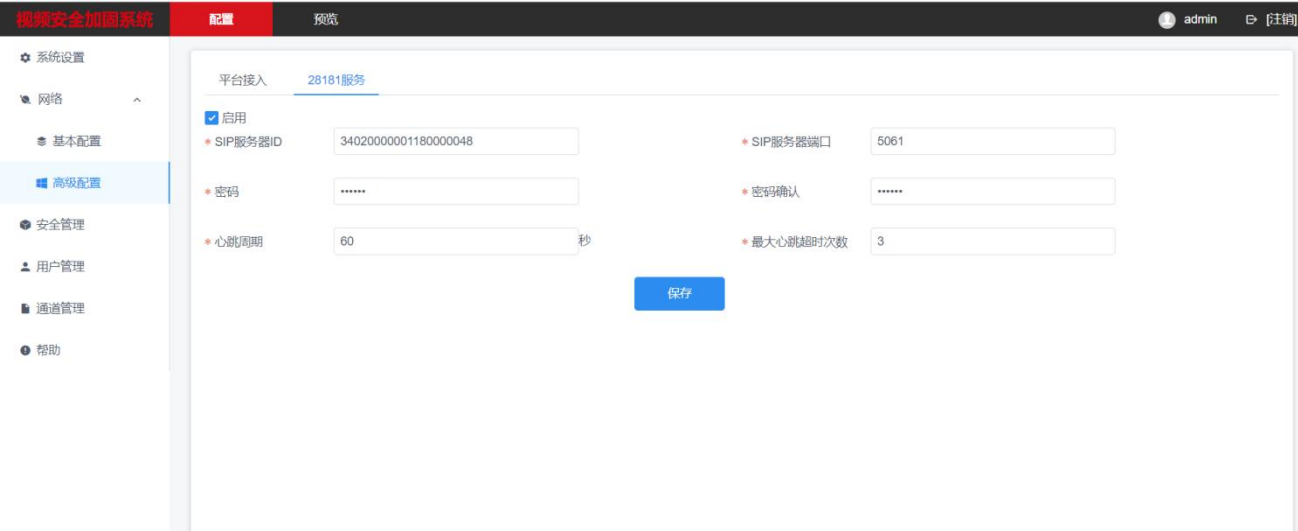


图 4-3 28181 服务



28181 服务界面配置参数说明：

- SIP 服务器 ID：本级安全加固终端的 SIP 服务器编号，设备唯一标识。
- SIP 服务器端口：本级安全加固终端 28181 服务的端口号，默认为“5061”，范围 1025-65535。
- 密码：前端视频设备在安全加固终端中的注册密码。初始密码是 123456，可修改，输入 6-12 位数字或字母。
- 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“两次密码输入不一致，请重新输入！”。
- 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。

- 最大心跳超时次数：心跳信息连续超时达到“最大超时次数”，则认为前端视频设备无法与安全加固终端建立连接。系统默认最大超时次数为 3 次，建议采用默认值，范围 3-255。

参数配置完成后单击“保存”完成参数配置。

通道相关信息：

呈现安全加固终端接入的前端视频设备的通道号，每个通道号下自动获取视频通道编码 ID（20 位数字）。当前端视频设备接通的情况下显示前端视频设备 ID，五网口视频安全转换器最多可接入四路前端视频设备。（在线状态是判断视频流是否接入成功）。如图 4-4 所示。

通道相关信息 >

通道号	视频通道编码ID	在线状态
D1	34020000001320000068	离线
D2	34020000001320000061	在线
D3	34020000001320000015	在线

图 4-4 通道相关信息

4.2.3 证书管理

选择“配置→网络→高级配置→平台接入”进入证书管理界面。证书管理界面包括证书请求创建、证书请求下载、证书请求删除、CA 证书、安装生成的证书、SIP 证书、CRL 证书撤销列表。如图 4-5 所示。

证书管理

说明: 请先保存平台信息后再安装证书

创建证书请求

创建

CN=34020000001180000045_1717012019110151132908,C=CN,ST=34,L=02,O=02,O=00

证书请求下载

下载

证书请求删除

删除

CA证书

ca.cer

浏览

安装

安装生成的证书

cert.cer

浏览

安装

SIP证书

slp.cer

浏览

安装

CRL证书撤销列表

crl.cer

浏览

安装

图 4-5 证书管理



单击“创建证书请求-创建”，创建设备证书，设备证书主体信息显示在按钮右边。

单击“证书请求下载-下载”，设备证书下载到本地，发给认证机构进行认证。

单击“证书请求删除→删除”，创建的证书被删除。

“CA 证书”，用户从 CA 服务中心下载 CA 根证书、SIP 平台证书、CRL 证书撤销列表。必须先安装 CA 根证书，其他证书才能安装，如果没有安装 CA 根证书，安装了其他证书，将出现错误提示：请先安装 CA 根证书。单击“浏览”，上传生成 CA 根证书的文件，单击“安装”，安装完成，提示“操作成功”。安装失败，提示“操作失败”。

“安装生成的证书”，单击“浏览”，上传生成安全加固终端的证书文件，单击“安装”，安装生成的证书，安装完成，提示“操作成功”。安装失败，提示“操作失败”。

“SIP 证书”，单击“浏览”，上传生成 SIP 证书的文件，单击“安装”，安装生成的证书，安装完成，提示“操作成功”。安装失败，提示“操作失败”。

“CRL 证书撤销列表”，单击“浏览”，上传生成 CRL 证书的文件，单击“安装”，安装生成的证书，安装完成，提示“操作成功”。安装失败，提示“操作失败”。

4.2.4TLS

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。TLS 加密通道有两种模式：TLS 客户端、TLS 服务端。

选择“配置→网络→高级配置→TLS 服务端”输入 TLS 服务端参数，勾选“启用”，即可启用 TLS 服务端加密功能，如图 4-6 所示。

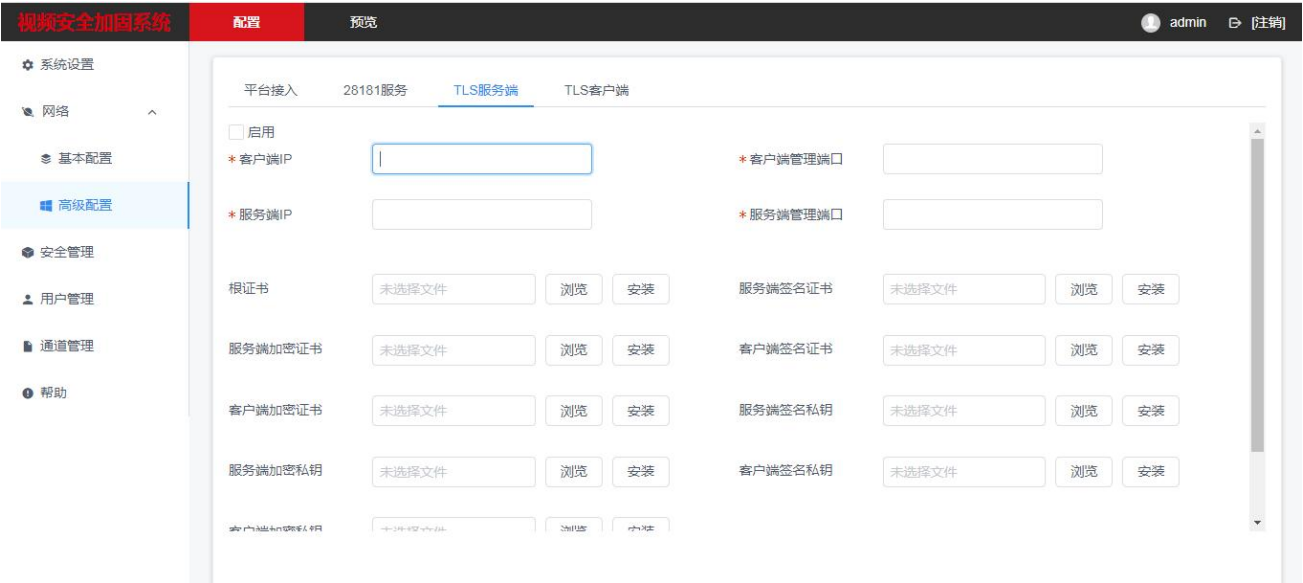


图 4-6 TLS 服务端



TLS 服务端界面配置参数说明：

客户端 IP：输入客户端 IP 地址。IP 地址须符合 IP 地址格式要求。

客户端管理端口：输入客户端管理端口，管理端口范围为 1~65535。

服务端 IP：输入服务端 IP 地址。IP 地址须符合 IP 地址格式要求。

服务端管理端口：输入服务端管理端口，管理端口范围为 1~65535。

证书导入：单击“浏览”，选择导入的证书文件，单击“安装”。安装导入的证书，提示“安装成功”，即完成证书导入成功。

选择“配置→网络→高级配置→TLS 客户端”输入 TLS 客户端参数，勾选“启用”，即可启用 TLS 客户端加密功能，如图 4-7 所示。

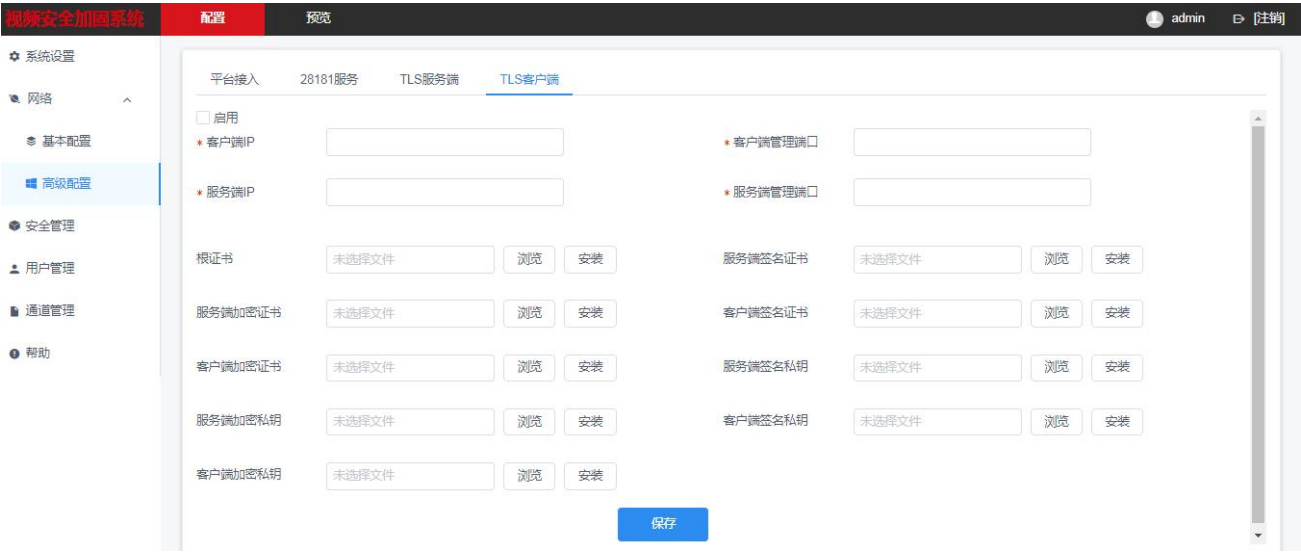


图 4-7 TLS 客户端



TLS 客户端界面配置参数说明：

客户端 IP：输入客户端 IP 地址。IP 地址须符合 IP 地址格式要求。

客户端管理端口：输入客户端管理端口，管理端口范围为 1~65535。

服务端 IP：输入服务端 IP 地址。IP 地址须符合 IP 地址格式要求。

服务端管理端口：输入服务端管理端口，管理端口范围为 1~65535。

证书导入：单击“浏览”，选择导入的证书文件，单击“安装”。安装导入的证书，提示“安装成功”，即完成证书导入成功。

5.安全管理

选择“配置→安全管理”进入用户 IP 接入黑名单界面。

您可以自行添加 5 个黑名单 IP 地址，添加完成后，单击“保存”，则添加的 IP 地址不能访问视频安全加固系统管理页面。如图 5-1 所示。

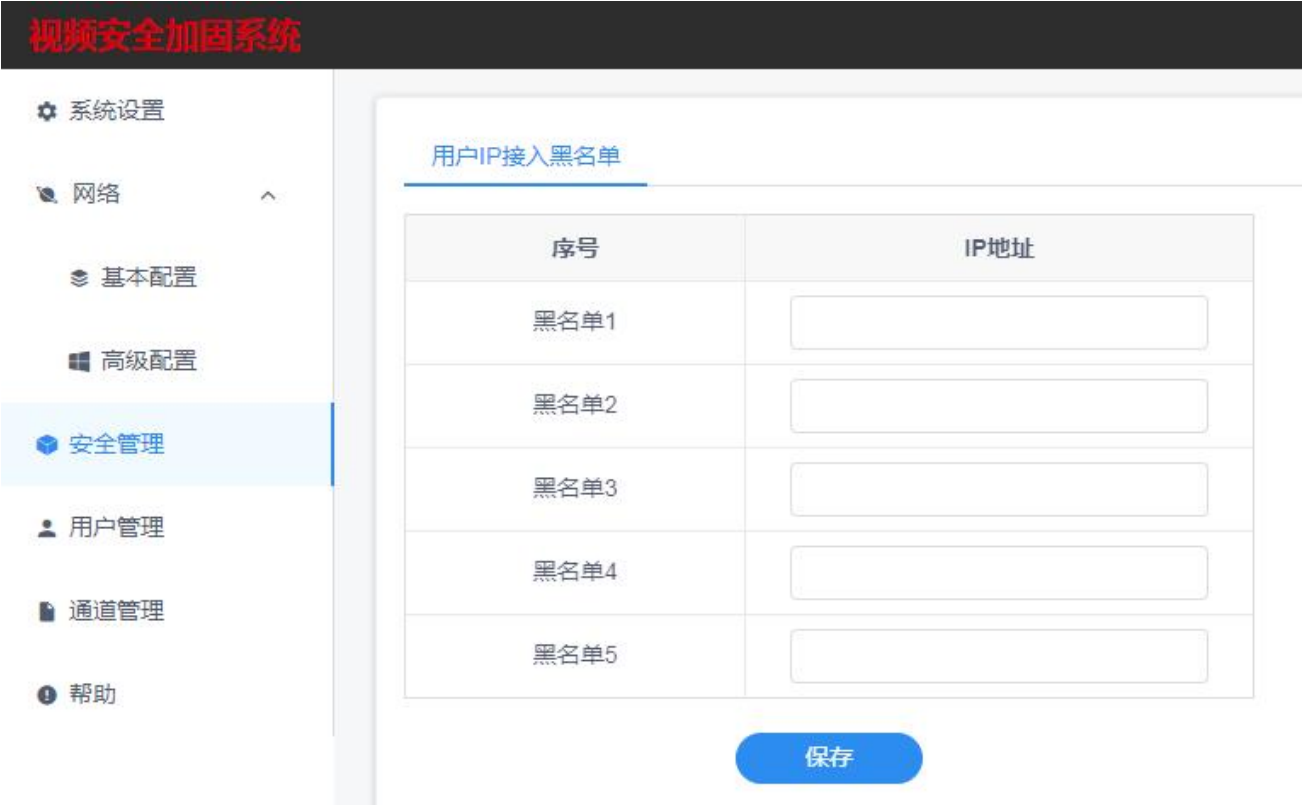


图 5-1 安全管理

6. 用户管理

选择“配置→用户管理”进入用户管理界面，可以对视频安全加固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，如图 6-1 所示。

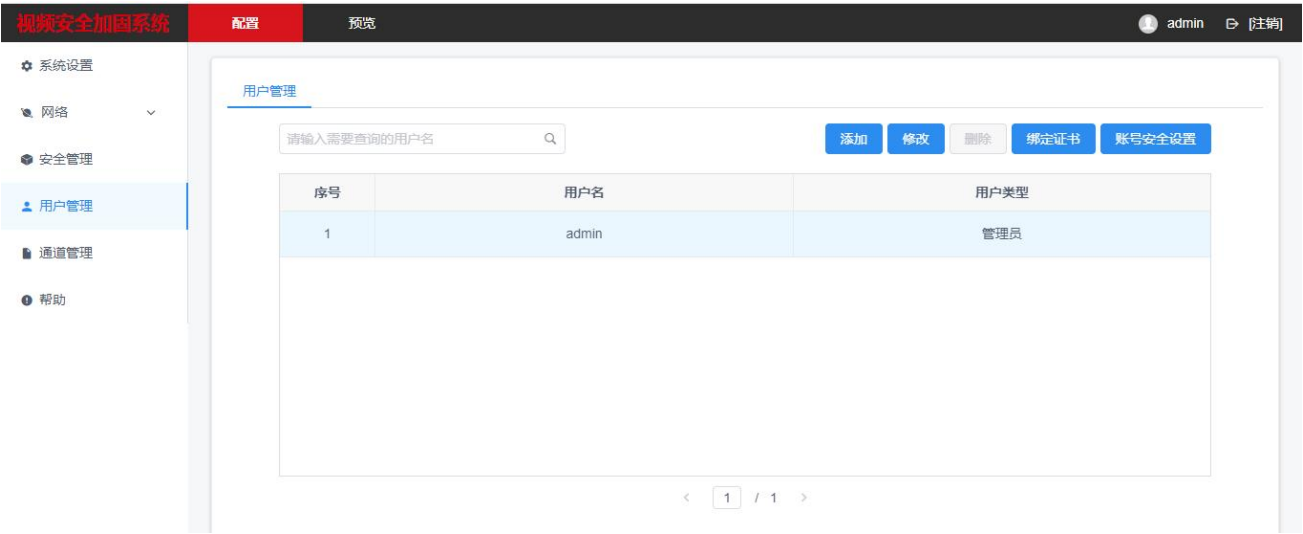


图 6-1 用户管理

6.1 用户添加

选择“配置→用户管理”，进入用户管理界面，单击界面上“添加”，弹出用户添加界面，如图 6-2 所示。

输入用户名、选择用户类型、密码（8-16 位数字或字母）、密码确认，选择权限后单击“确定”，用户添加成功。



图 6-2 用户添加



注意

- 为了提高产品网络使用的安全性，请您定期更改用户名的密码，建议每 3 个月进行一次更新维护。如果产品在较高安全风险的环境中使用，建议每月或每周进行一次更新维护。
- 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，设置密保，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。

6.2 用户修改

选择“配置→用户管理”，选择需要修改的用户名，单击“修改”，进入用户修改界面。此界面可以修改“密码”和“用户类型”。密码设置规则请参见用户添加的步骤。如图 6-3 所示。



图 6-3 用户修改

6.3 用户删除

管理员选择“配置→用户管理”，单击需要删除的用户点击“删除”，提示“是否删除该用户”，单击“确定”，提示“删除成功”。单击“取消”，提示“已取消删除”。不可删除管理员用户。如图 6-4 所示。

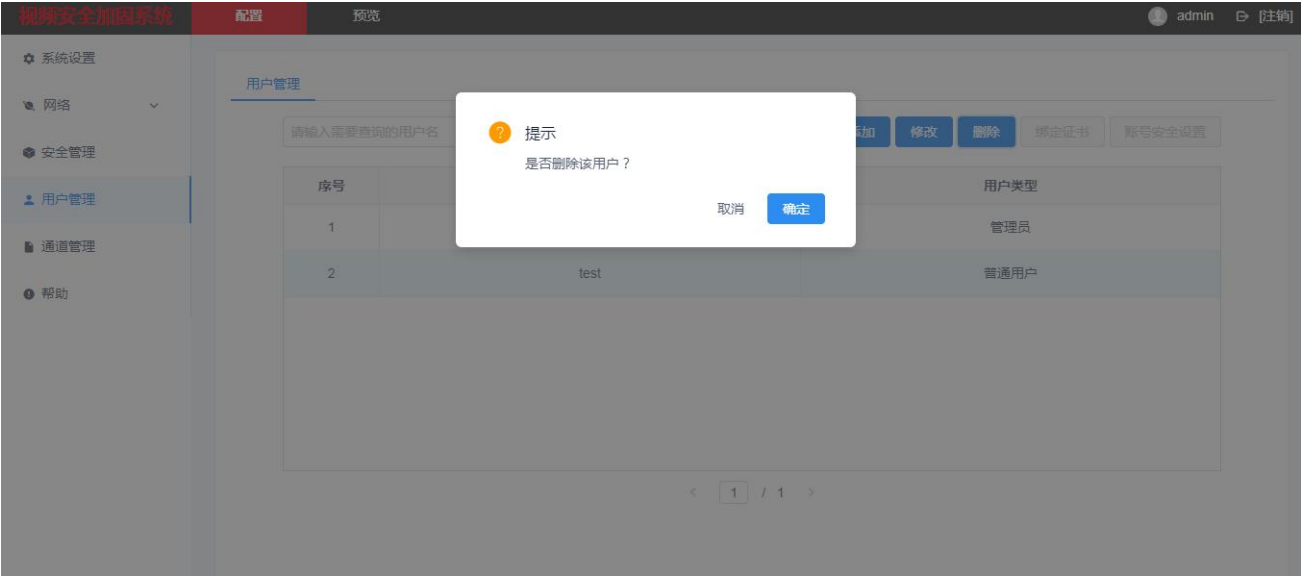


图 6-4 用户删除

7.通道管理

选择“配置→通道管理”，进入“通道管理”界面，通道管理界面显示添加的前端设备信息。显示内容包括设备编码、设备 IP、设备 MAC、端口、状态（在线/离线）、安全性（强/中/弱）、协议类型、操作（修改/删除）。（这个状态是现实摄像机是否成功接入到视频安全转换器）如图 7-1 所示。



图 7-1 通道管理

7.1 设备添加

选择“配置→通道管理”，单击界面上“添加”，弹出数字通道配置界面，如图 7-2 所示。

输入安全加固终端接入的前端视频设备的详细信息，包括设备的协议类型、设备名称、设备编码、MAC 地址（必须小写）、IP 通道地址、管理端口、用户名、密码、密码确认、传输协

议。输入完成后单击“确定”，提示“设备添加成功”。

数字通道配置

* 协议类型

请选择

* 设备名称

请输入设备名称

* 设备编码

请输入设备编码

* MAC地址

请输入MAC地址

* IP通道地址

请输入IP通道地址

* 管理端口

请输入管理端口

* 用户名

请输入用户名

取消

确定

图 7-2 设备添加



说明

协议为 RTSP，百度查找相机的 RTSP 地址，以海康相机为例说明。

海康相机 RTSP 地址格式如下：

URL 规定：

rtsp://username:password@<ipaddress>/ch<number>/<streamtype>

路径后面不能有空格、回车等符号，否则会连接失败。

举例说明；

主流码取流：

rtsp://admin:anwei888@192.168.0.68:554/h264/ch1/main/av_stream

子流码取流：

rtsp://admin:anwei888@192.168.0.68:554/h264/ch1/sub/av_stream

加固系统中主流码资源路径写 **h264/ch1/main/av_stream**

子流码资源路径写 **h264/ch1/sub/av_stream**

如果是 H265 码流，将 H264 码流替换成 H265 即可。海康相机默认 RTSP 端口为 554，根据海康相机界面 RTSP 端口修改即可。

7.2 设备修改

选择“配置→通道管理”，单击“修改”，进入设备修改界面。如图 7-3 所示。

数字通道配置

* 协议类型 GB28181

* 设备名称 61

* 设备编码 34020000001320000061

* MAC地址 ec:c8:9c:7d:46:be

* IP通道地址 192.168.0.61

* 管理端口 5061

* 用户名 admin

取消 确定

图 7-3 设备修改

7.3 设备删除

选择“配置→通道管理”，单击需要删除的设备行对应的“删除”，提示“是否删除该设备”，

单击“确定”，提示“删除成功”。单击“取消”，提示“已取消删除”。如图 7-4 所示。通道管理界面的设备删除后，“网络→高级配置→通道相关信息”界面设备自动删除。

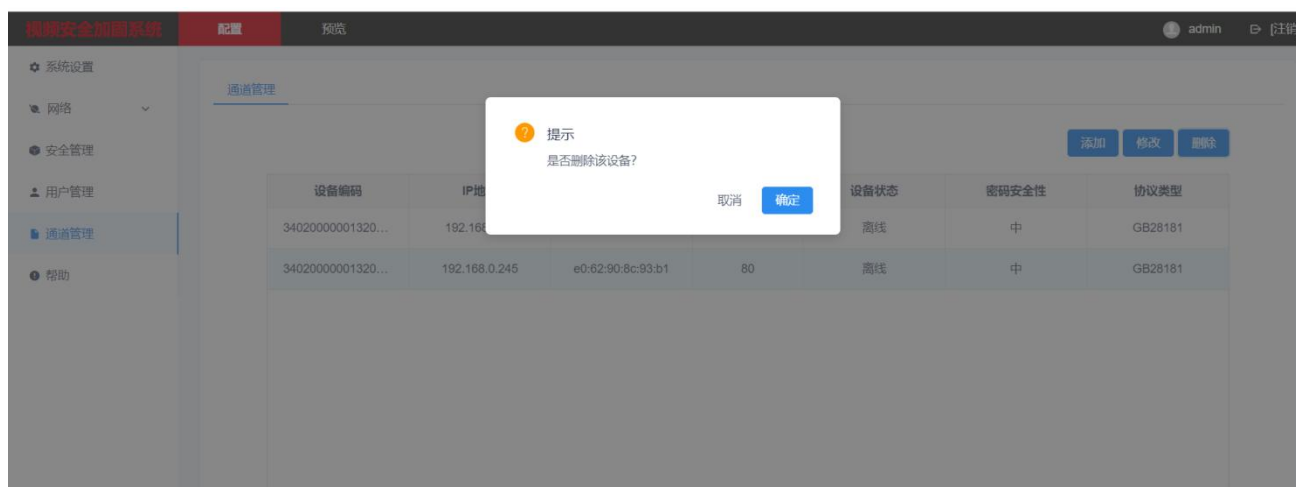


图 7-4 设备删除

8. 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）。预览页面支持视频视频抓图、视频录制和全屏预览。界面如图 8-1 所示。



图 8-1 预览界面

8.1 预览工具栏

视频预览：单击在线视频列表中任意一台设备，画面播放区域显示监控画面。

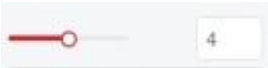
图标	名称	功能说明
	全部开始预览	点击“全部开始预览”按钮，在线列表视频开始播放。再次点击，预览播放停止。
	画面布局	画面播放区域左下角的切换布局按钮，可单屏预览也可多屏预览。
	抓图	可对预览窗口中的实时画面进行手动抓拍。点击“抓图”按钮，抓图为.png 的文件被下载。
	全部开启录像	首次单击开始录像，再次单击录像结束，并自动保存到已设置路径。录像文件“XX.gif”被下载。
	全屏	在全屏模式下显示实时视图。按 Esc 键，退出全屏模式。

8.2 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。

8.2.1 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。

8.2.2 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。

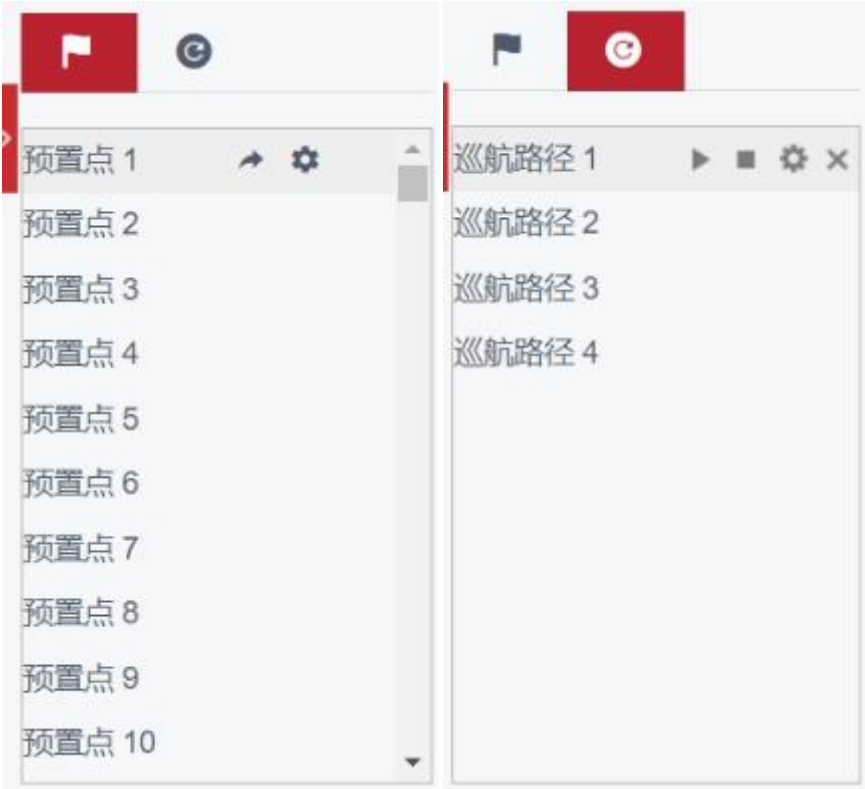


图 8-2 预置点/巡航路径



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“”，可设置预置点位置。

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。	