

八路视频安全转换 (GB 35114 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

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,请您严格遵循使用的法律。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。
- 如本手册内容与试用的法律相冲突,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-300。

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。
<u>▲</u> 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。

# 11章

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,请你加强个人信息几数据安全保护。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.	产品说明	. 7
1.	产品功能	. 7
1.	产品特性	. 8
1.	产品参数	. 8
1.	产品外观	. 9
2. ‡	作须知	10
2.	系统登录与退出	10
2.	主界面说明	11
3. 🕺	统参数设置	12
3.	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. 🕅	络参数设置	16
4.	基本配置	16
	4.1.1 IP 配置	16
	4.1.2 路由配置	16
	4.1.3 端口转发	17
4.	高级配置	18
	4.2.1 平台接入	18
	4.2.2 28181 服务	19
	4.2.3 证书管理	21
5. 🗦	全管理	22
<b>6.</b> 月	户管理	22
6.	添加用户	23

(	5.2 修改用户	. 24
(	5.3 删除用户	. 25
7.	通道管理	. 26
-	7.1 添加设备	. 26
-	7.2 修改设备	. 27
-	7.3 删除设备	. 28
8.	预览	. 29
9.	帮助	. 29

## 1. 产品简介

#### 1.1 产品说明

AWS-Model-310C 八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;可以为己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 GB35114-2017 的设备 安全性提升。

### 1.2 产品功能

支持 8 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 28181、ONVIF 与 GB 35114 互转

转换器融合国产商用密码芯片,支持 SM1/2/3/4 算法,支持数字证书、会话密钥的安全存储

支持网络摄像机常用的 SIP、HTTP、RTSP 等协议的安全处理

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 8 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 IP、端口、MAC 地址、协议指纹等多种方式的前端设备安全绑定

设备支持采用门卫或并接方式部署,支持转发协议配置,只允许指定协议通过,配置可以 通过后端平台进行设置

支持国密 SSL 通道构建,支持与后端管理平台构建国密 SSL 通道,支持非视频数据的国密

SSL 通道安全防护,单台设备支持不少于 8 条国密 SSL 通道建立

设备配置有日志管理服务功能,可以对设备的异常操作,如网线拔除、相机掉线等异常情况进行报警,报警信息支持在后端管理平台查看

支持软件在线更新,可扩展支持更新固件/软件的完整性校验

支持对接公安部视频密码平台

### 1.3 产品特性

本产品采用"9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 GB35114-2017 (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,采用 GB 35114 C 级方式实现对码流的加密防护。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。

## 1.4 产品参数

规格/型号		AWS-Model-310C		
	接入压缩标准	H.264、H.265		
视频	输出压缩标准	SVAC2.0		
	支持视频路数	八路		
	H.265 编码类型	Main Profile		
	H.264 编码类型	Main Profile/High Profile		
	音频编码	G711U/G711A		
切肥	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			
	以太网	9个 RJ-45 接口, 10M/100M 自适应			
网络	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			
	尺寸	210mm*160mm*30mm			
	电源	DC12V 2A			
一般	工作温度	-30°C~+60°C			
规范	工作湿度	10%~90%			
	功率	<15W			
	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 DC12V 电源
2	WAN 网络接口	接入后端网络设备
3	LAN 网络接口	接入前端视频设备
4	电源指示灯	设备通电时常亮
5	WAN 网络指示灯	本机通电并接入网络设备后,左灯橙色常 亭,左灯绿色闪烁
		宂, 石月寒巳内脉

## 2. 操作须知

2.1 系统登录与退出

登录系统

# 1 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账号管理员账号,用户名:admin,密码: Admin@12345#。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。

本系统支持安全问题的方式重置密码,管理员登录系统后,可先配置安全问题,通过安全问题的方式重置系统密码。

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 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1] "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。

视频安全加固系统	配置	预党			1 admin & [注销]
✿ 系统设置	甘大信白		ゲエスを		
<b>@</b> 网络 ~	金仲间思	可问闻直 开级距产 口心	大丁设副		
● 安全管理	产品名称	八路视频安全转换器	设备安全等级	GB35114	
▲ 用户管理	公司名称	北京安为科技有限公司	设备序列号	10000001	
▶ 通道管理	设备型号	AWS-Model-300	Web版本	V1.1.3	
● 帮助	生产厂商	北京安为科技有限公司	主版本	V3.1.12	
4					Þ

图 2-2 主页面

# 1 说明

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。

视频安全加固系统	配置	预览				🔹 admin	日注销
✿ 系统设置							
◙ 网络 ~	量本信息 	时间配置 并级维护 日志	关于设备				
● 安全管理	产品名称	八路视频安全转换器		设备安全等级	GB35114		
▲ 用户管理	公司名称	北京安为科技有限公司		设备序列号	10000001		
▶ 通道管理	设备型号	AWS-Model-300		Web版本	V1.1.3		
● 帮助	生产厂商	北京安为科技有限公司		主版本	V3.1.12		
4	_						

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。 AWS-Model-310C 八路视频安全转换器(GB 35114 C 级)•操作手册

视频安全加固系统	配置	预党	』 admin ເ⊖ [注销]
✿ 系统设置			
<b>箋 网络 ~</b>	基本信息	时间截置  升级维护  日志  关于设备	
● 安全管理	时区	(GMT+08:00)北东、乌鲁木齐、新加坡 ~	
▲ 用户管理	NTP校时		
	服务器地址	ntp.aliyun.com	
	NTP端口	123	
● 帮助	校时时间间隔	1440 分軸 2016	
	120303F3F3F3F8		
	◎ 手动校时		
	设备时间	2024-08-02 10:37:48	
	设置时间	2024-08-02 10:37:48	
	保存		

图 3-2 时间设置

# 1 说明

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可选:

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。

视频安全加固系统	配置 一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一
✿ 系统设置	
💘 网络 🗸 🗸	
● 安全管理	重启重新启动设备
≗ 用户管理	恢复默认值
▶ 通道管理	恢复出厂设置恢复设备参数到出厂设置
● 帮助	升级
	升级文件末选择文件 浏览 升级
	*说明:设备重启过程需要1-10分钟,请不要关闭电源。

图 3-3 升级维护

i 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,升级完成后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。 AWS-Model-310C 八路视频安全转换器(GB 35114 C 级)•操作手册

	基本信息	时间配置 升级维护	日志 关于	F设备			
网络 ~							
全管理	全部 ~	火英型: 全部 ~	开始时间:	2024-08-01 00:00:00	结束时间: 2024-0	8-02 23:59:59 📋	查询  导出
」户管理	序号	时间	主类型	次类型	日志通道	用户名	IP地址
道管理	1	2024-08-02 10:3	操作	配置时间		admin	192.168.0.124
助							

图 3-4 日志

# i 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 按键的日志信息。

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,主要对视频安全转换器 进行详细说明。如图 3-5 所示。

<ul> <li>◆ 系统设置</li> <li>▲ 网络</li> <li>▲ 本产品是一款面向已建现频监控系统,实施*利旧性安全改造的产品,我们的产品形态可实现单路,四路和八路前端据</li> <li>● 安全管理</li> <li>▲ 本产品是一款面向已建现频监控系统,实施*利旧性安全改造的产品,我们的产品形态可实现单路,四路和八路前端据</li> <li>像头的安全加固改造,四进一出安全转换器最多支持四路摄像机间时接入,该产品采用国家商用密码算法芯片和高性能嵌入</li> <li>式处理器,对照GB35114-2017国家标准研发,可为已袭安防视频监控设备提供便利的设备身份认证,视频流加密,视频关键检密各等安全功能。</li> <li>▲ 本产品可广泛应用于实际,保密、公安等对视频安全防护要求软高的行业和场所,可以对无安全防护措施的网络摄像机</li> </ul>	销]
風外信息         町川配査         井坂理炉         日志         天井设備           ● 内培         町川配査         井坂理炉         日志         天井设備           ● 次合         本产品是一款面向已建现频监控系统,实施*利旧*性安全改進的产品、我们的产品形态可实现单路、四路和八路前端据            ● 安全管理         像头的安全加固改造。四进一出安全转换器最多支持四路摄像机间时接入。该产品采用国家商用密码算法芯片和高性能嵌入            1. 用户管理               1. 開户管理                1. 通道管理	
本产品是一款面向已建视频监控系统,实施 和II "住安全改造的产品,找们的产品形态可实规单路,凹路和//路前颠簸       ● 安全管理     像头的安全加固改造,四进一出安全转换器最多支持四路摄像机同时接入。该产品采用国家商用密码算法芯片和高性影嵌入       式处理器,对照GB35114-2017国家标准研发,可为已接安防视频监控设备提供便利的设备身份认证、视频流加密、视频关键缺签名等安全功能。       ▲ 用户管理     键帧签名等安全功能。       ● 通道管理	
・用户管理     式处理器, 对照GB35114-2017国家标准研发, 可为已读安防视频监控设备提供便利的设备身份认证、视频流加密、视频关键就签名等安全功能。       ・通道管理     罐帧签名等安全功能。       ・通道管理     地方用于军队、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	
▲ 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	
设备提供思想和的安全加固。 伊爾廷提斯特(BB35114-2017)的设备安全性保持	
4	•

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

#### 4.1.1 IP 配置

选择"配置→网络→基本配置"进入"IP 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、LAN 口 IPv4 地址、LAN 口子网掩码、 LAN 口物理地址、首选 DNS 服务器、备用 DNS 服务器,如图 4-1 所示。

视频安全加固系统	配置	预览			🔹 admin	₿[注销]
✿ 系统设置	The second secon	an an unit of the second second				
◙ 网络 ∧	IP配置 器	各由配置 端口转发				
◎ 基本配置	模式切换	门卫模式	设备IPV4地址	192.168.0.42	测试	
■ 高级配置	网卡类型	自适应	IPv4子网掩码	255.255.255.0		
● 安全管理	物理地址	00:11:22:33:44:55	IPv4默认网关	192.168.0.1		
▲ 用户管理	LAN口配置					
▶ 通道管理	设备IPv4地址	192.168.1.1	IPv4子网掩码	255.255.255.0		
<ul> <li>帮助</li> </ul>	物理地址	00:11:22:33:44:56				
	DNS服务器配置					
	首选DNS服务器	223.5.5.5	备用DNS服务器	8.8.8.8		
	RA					
	URD -					
4						

图 4-1 IP 配置

1 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。

LAN 口 IPv4 不可配置为 172.16.30.1, 该 IP 已被内部占用。

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。

#### 4.1.2 路由配置

选择"配置→网络→基本配置"进入"路由配置"页面。主要配置内容:目的网络地址、

子网掩码,如图 4-2 所示

视频安全加固系统	配置	预览			① admin & [注销]
✿ 系统设置		86-1-37-99 Jul - 1-4-112			
◙ 网络 ^	PWE	始田配直 靖山牧久			
● 基本配置		日本网络地址	了网络门	添加	
■ 高级配置		日期國籍地址	计例用问	IXTE	
● 安全管理		192.168.3.1	255.255.255.0	保存删除	
▲ 用户管理					
▶ 通道管理					
● 帮助					
4					-

图 4-2 路由配置

i 说明

在路由配置界面,参数配置完成后单击"保存"完成参数配置,点击"删除"即可删除该路由。

## 4.1.3 端口转发

选择"配置→网络→基本配置"进入"端口转发"页面。主要配置内容: 名称、协议、外 部端口、内部 IP 地址、内部端口,如图 4-3 所示。

系统设置 网络 へ	IP配置 路由配置	端口转发					
≥ 基本配置	名称	协议	外部端口	内部IP地址	内部端口	漆加操作	
■ 高级配置	77	TCP+UDP ~	8090	192.168.1.77	80	保存 删除	
用户管理							
通道管理							
帮助							

#### 图 4-3 端口转发

# 1 说明

在端口转发界面,名称为设备名称,可区分不同设备即可,协议可选 TCP/UDP/TCP+UDP, 外部端口为安全转换器转发后的端口,内部 IP 地址为相机的 IP 地址,内部端口为相机的服务 端口。

参数配置完成后单击"保存"完成参数配置,点击"删除"即可删除该端口转发信息。

#### 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"。

i 说明

视频设备安全加固终端支持 GB/T28181 和 GB/T35114 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 GB/T 35114 的协议转换,并接入上级 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 4-4 所示。

勾选"启用"前,需完成证书配置、同步时间、相机视频已推到转换器,若"启用"后增加了相机视频,需重新"启用"。

机频安全加固系统	配置	预览			
✿ 系统设置	平台接入 2	8181服务			
◙ 网络 ∧	✓ 启用				
◎ 基本配置	平台接入协议	GB 35114-2017	*本地SIP端口	5060	
■ 高級配置	* SIP服务器ID	340200000200000221	* SIP服务器域	3402000000	
● 安全管理	* SIP服务器地址	192.168.0.221	*SIP服务器端口	5061	
≗ 用户管理	* SIP用户认证ID	3402000001180000021	* 注册有效期	3600	秒
▶ 通道管理					
● 帮助	* 心跳周期	60 秒	* 最大心跳超时次数	3	

#### 图 4-4 平台接入

# i 说明

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 3600-100000。
- 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。

#### 4.2.2 28181 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 4-5 所示。

视频安全加固系统	配置	预览				٥
✿ 系统设置	Table					
<b>2 网络 ^</b>	+台接入	26181服务				
\$ 基本配置	* SIP服务器ID	3402000001180000021		* SIP服务器端口	5061	
■ 高级配置	* 密码			* 密码确认	•••••	
● 安全管理	* 心跳周期	3600	秒	* 最大心跳超时次数	250	
▲ 用户管理						
▮ 通道管理				<del>探存</del>		
❹ 帮助		_				

#### 图 4-528181 服务

#### i 说明

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:

呈现视频安全转换器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,八路视频安全转换器 最多可显示八路前端视频设备。(在线状态是判断视频流是否接入成功)。如图 4-6 所示。



图 4-6 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 4-7 所示。

视频安全加固系统	配置	预览						
✿ 系统设置	平台接入	28181服	务					
◙ 网络 ^	证书管理							
\$ 基本配置	说明:请先保存	平台信息后	再安装证书					
■ 高级配置	创建证书请求	创建	CN=340200000011800000	21_17170120	19120149093	2906,C=CN,S	T=34,L=02,L=	=00,O=02,O=00
▲ 六么 <sup>œт</sup> ⊞	证书请求下载	下载						
♥ 安王官埋	证书请求删除	删除						
≗ 用户管理	CA证书		ca.cer	浏览	安装			
■ 通道管理	安装生成的证书		cert.cer	浏览	安装			
0 帮助								
	SIP证书		sip.cer	浏览	安装			
	CRL证书撤销列录	表	未选择文件	浏览	安装			

图 4-7 证书管理

# i 说明

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"。

### 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。

	配置	预览		
✿ 系统设置	田山口按入	型交前		
Ng 网络 V	7117 10 1327 (3			
♥ 安全管理	L	<b></b> 字号	IP地址	
▲ 用户管理	黑	名单1		
<ul> <li>■ 通道管理</li> <li>● 帮助</li> </ul>	黑	名单2		
	黑	名单3		
	黑	名单4		
	黑	名单5		

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。

视频安全加固系统	配置 预览		』 admin ⊖ 注销
✿ 系统设置			
<b>@</b> 网络 ~		2	
♥ 安全管理	请输入需要重询的用户名	q	<b>添加 终女 國際</b> 研定证书 舞号安全设置
▲ 用户管理	序号	用户名	用户类型
▶ 通道管理	1	admin	管理员
◆ 邦田1	2	test1	普通用户
U TPAJ			
		< 1	71 >
•			•

图 6-1 用户管理

## 6.1 添加用户

选择"配置→用户管理",进入用用户管理界面,单击界面上"添加",弹出添加用户界面, 如图 6-2 所示。

输入用户名、选择用户类型、密码(6-12 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。

和频安全加固系统	配置 预	用户添加	×admin D→ [注销]
◆ 系统设置			
<b>观</b> 网络 ~	用户管理	* 用户名:	请输入用户名
● 安全管理		* 用户类型:	☆ ■●●● 「「「「」」 「「」」 「「」」 「「」」 「」」 「「」」 「」」 「
<b>1</b> 用户管理	序号	<b>*</b> 密码:	開始入空四
▶ 通道管理	1		管理员
<b>9</b> 帮助	2	10.000	8-16位,只能用数字、小写字母、大写字母、特殊字符的两种及以上组合 普通用户
		*密码确认:	请称从 <b>驾</b> 归
		权限:	2 全部权限 11/11 □ 已造权限 0
			☑ 升级 ▲ 列版为空
			取消 确定
		-	

图 6-2 添加用户



- 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。

#### i 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 6-12 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 修改用户

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"、"用户类型"、"用户权限"。密码设置规则请参见添加用户的步骤。如 图 6-3 所示。

修改					×
<mark>*</mark> 用户名:	test1				
*人员类型:	普通用户				~
∗ 新密码:					
*确认新密码:					
权限:	全部权限         0           列表为空	< >	<ul> <li>已选权限</li> <li>升级</li> <li>格式化</li> <li>重启</li> <li>配置IP</li> <li>配置时间</li> </ul>	11	
				取消	确定

#### 图 6-3 修改用户

## 6.3 删除用户

管理员选择"配置→用户管理",单击需要删除的用户行对应的"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。

	添加用户 操作 3 设置密保 修改	操作	消	3	提示 是否删除该用户?	•	唐输入需要查询的用户名 用户名 admin	
test1 普通用户 修	修改 删除	修改		普通用户			test1	

图 6-4 删除用户

## 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)。(设备状态为摄像机是否成功接入到视频安全转换器)如图 7-1 所示。

・ 余総理       ・ </th <th>视频安全加固系统</th> <th>配置</th> <th>预览</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>I admin</th> <th>⊖ [注销]</th>	视频安全加固系统	配置	预览							I admin	⊖ [注销]
原始       ・         ● 交金館理       ・ <td< td=""><td>✿ 系统设置</td><td>1211-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-</td><td>-</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td<>	✿ 系统设置	1211-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-	-								
● 安全管理       第二       日戸管理       10       10       10       10       10       26       10       10       28       10	<b>义</b> 网络 V	通過官;	#								
・通道管理       ・通信       <	● 安全管理								添加	修改 删除	
通道管理       test       3402000       192.168.1       34:2d:23:4       80       高线       弱       GB28181         ● 帮助	▲ 用户管理		设备名称	设备编码	IP地址	设备MAC	管理端口	设备状态	安全性	协议类型	
● 帮助	▶ 通道管理		test	34020000	192.168.1	34:2d:23:4	80	离线	55	GB28181	
	● 帮助										

图 7-1 通道管理

## 7.1 添加设备

选择"配置→通道管理",单击"添加",弹出添加设备界面,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

数字诵道配置

协议。输入完成后单击"确定",提示"设备添加成功"。最多可添加8个设备通道。

×

*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 添加设备

## 7.2 修改设备

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。

视频安全加固系统	配置 预览						i admin ⊖ [	注销]
✿ 系统设置	通道管理	数字诵道配置		×				
<b>@</b> 网络 ~								
● 安全管理		*协议类型	GB28181	~		添加	修改副除	
▲ 用户管理	设备名称	*设备名称	test		设备状态	安全性	协议类型	
▶ 通道管理	test	* 设备编码	3402000001320000001		离线	弱	GB28181	
● 帮助		* MAC地址	34:2d:23:43:da:d3					
		* IP通道地址	192.168.1.77					
		*管理端口	80					
		* 用户名	admin					
			取消	确定				

图 7-3 修改设备

## 7.3 删除设备

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。

视频安全加固系统	配置	预览					🛓 admin (	∋ [注销]
✿ 系统设置								
■ 网络 →	通追管埋					Steba	ASIA TIL	
● 安全管理			是否删除该设备?			AKUL		
▲ 用户管理		设备名称 设	简	取当	设备状态	安全性	协议类型	
D 通道管理		test 3402	20	-RATE	商线	弱	GB28181	
0 帮助								

### 图 7-4 删除设备

## 8. 预览

选择"预览",双击左侧视频通道,即可视频播放,预览最多支持四分屏播放。选择视频 通道,点击右侧云台控制的属性按钮,可对支持云台控制的摄像机云台操作,如图 8-1 所示。 点击视频画面下方按钮,可开启全部预览、分屏、画面尺寸、抓图、视频录像操作。



图 8-1 预览

## 9. 帮助

选择"配置→帮助",系统会跳转到新增的联机帮助页面,主要介绍每个菜单栏的功能及 其操作,如图 9-1 所示。

联机帮助	
■ 登录	
✿ 系统设置	登录 步骤1:在浏览器地址栏中输入本产品的IP地址,单击【回车】,将弹出本产品登录界面,
◙ 网络	步骤2:在登录界面输入"用户名"和"密码",单击"登录",将弹出本产品的"主界面"。
● 安全管理	
<ul> <li>田白管理</li> </ul>	

图 9-1 帮助