安全智能视频一体化服务系统

产品使用手册

2022 年 02 月

目录

1 本文标志 1

2 环境保护 1

3 安全 2

4 设备安装 4

4.1 SIVS708 4

4.1.1 设备正视图 4

4.1.2 前面板 LED 指示灯和按键 5

4.1.3 产品后视图 5

4.1.4 设备外形尺寸 6

4.1.5 机箱内部结构 6

4.1.6 背板快速参考 8

4.1.7 SATA 设备顺序 8

4.1.8 热插拔 SATA 硬盘驱动器选件 9

4.2 SIVS724 10

4.2.1 设备视图 10

4.2.2 设备上架安装 11

4.2.3 安装硬盘 12

4.2.4 磁盘管理（RAID）界面 14

4.2.5 创建 RAID 15

4.2.6 设置热备盘 16

4.2.7 创建 NASLUN 17

5 环境要求及准备 19

5.1 空间要求与通风要求 19

5.2 温度要求 20

5.3 电源要求 20

5.4 电气接地要求 21

5.5 机架/柜警告及要求 21

6 故障排除 23

6.1 预诊断步骤 23

6.2 症状信息 23

6.3 做好服务器诊断的准备工作 24

6.4 系统故障排除 24

6.4.1 系统启动失败故障排除 24

6.4.2 外部连接故障排除 24

6.4.3 USB 设备故障排除 25

6.4.4 串行 I/O 设备故障排除 25

6.4.5 受损系统故障排除 25

6.4.6 系统电池故障排除 26

6.4.7 电源设备故障排除 26

6.4.8 冷却问题故障排除 26

6.4.9 系统内存故障排除 27

6.4.10 处理器故障排除 28

7 更换系统电池 28
8 静电释放 30
8.1 防止静电释放 30
8.2 防止静电危害的接地方法 30
9 SIVS 登录 31
9.1 控件安装和卸载 31
9.1.1 控件安装 32
9.1.2 控件卸载 33
9.2 密码登录 33
9.3 USBkey 登录 34
9.4 版本确认 38
9.4.1 版本确认 38
9.4.2 版本升级 38
9.5 检查系统状态及授权信息 39
10 SIVS 授权申请 40
10.1 确认授权信息 40
10.2 复制国标编号 41
10.3 生成授权信息文件 42
10.4 发送授权申请邮件 44
10.5 授权文件上传 44
10.6 确认授权信息 45
11 SIVS 添加相机及其他配置 47

11.1 网络配置 47
11.2 SIVS 国标 ID 等信息及证书 48
11.2.1 SIVS 国标 ID 等信息的获取及修改 48
11.2.2 SIVS 证书的申请，获取及修改 49
11.3 GB35114 设置（添加相机） 51
11.3.1 系统自动添加相机 52
11.3.2 添加相机证书 54
11.3.3 前端相机注册成功 57
11.3.4 前端相机更改安全等级 59
11.3.5 前端相机名称修改 60
11.4 存储 61
11.4.1 存储管理 61
11.4.2 计划配置 62
12 实时浏览 63
12.1 实时视频 63
12.1.1 实时视频浏览 63
12.1.2 前端相机的安全等级显示 66
12.1.3 视频浏览基本功能 68
12.1.4 云台功能 70
12.2 视频轮巡 71
12.2.1 添加视频轮巡 71
12.2.2 修改视频轮巡 72

12.2.3 删除视频轮巡 72

12.2.4 应用轮巡 72

13 录像回放 73

13.1 录像回放功能 73

13.2 前端相机的录像安全等级显示 74

13.3 录像下载功能 74

14 解码设备配置与投屏 74

14.1 系统自动添加解码设备 74

14.2 添加解码设备证书 76

14.3 解码设备注册成功 79

14.4 解码设备更改安全等级 81

14.5 解码设备名称修改 82

15 解码控制 83

15.1 添加解码设备 83

16 SIVS 对接 VISS 平台 83

16.1 SIVS 以 GB/T28181 协议接入 VISS 83

16.1.1 SIVS 配置 83

16.1.2 VISS 配置 85

16.2 SIVS 以 GB35114 安全功能方式接入 VISS 85

16.2.1 SIVS 配置 86

16.2.2 VISS 配置 87

附录一、相机配置 88

附录二、相机证书的导入 94

附录三、USBkey 证书的导入 97

附录四、USBkey 证书的验证及导出 99

附录五、解码设备配置及证书配置 104

附录六、国标 ID 简易介绍 108

附录七、使用注意事项 110

1 本文标志

本文采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
说明	对操作内容的描述进行必要的补充和说明。

2 环境保护

本产品符合关于环境保护方面的设计要求，产品的存放、使用和弃置应遵照相关国家法律、法规要求进行。

3 安全

在安装本产品之前，请仔细阅读安全信息。

一、 警告

电源、电话和通信电缆的电流具有危险性。

为避免电击危险：

- 请勿在雷暴天气期间连接或断开任何电缆的连接，安装、维护或重新配置本产品。
- 将所有电源线连接正确且采用接地的电源插座。
- 将所有要连接到本产品的设备连接到正确连线的插座。
- 尽量仅用单手连接或断开信号电缆的连接。
- 切勿在有火灾、水灾或房屋倒塌迹象时开启任何设备。
- 除非安装和配置过程中另有说明，否则请在打开设备外盖之前断开已连接的电源线、远程通信系统、网络和调制解调器等设备。
- 对本产品或连接的设备执行安装、移动或打开外盖的操作时，请按下表所述连接和断开电缆连接。

要连接，请执行以下操作：	要断开连接，请执行以下操作：
1. 关闭所有设备。	1. 关闭所有设备。

2. 首先将所有电缆连接至设备。 3. 将信号电缆连接至接口。 4. 将电源线连接至插座。 5. 开启设备。	2. 首先从插座上拔出电源线。 3. 从接口上拔出信号电缆。 4. 从设备上拔出所有电缆。

二、 注意

更换系统电池时，请使用同类电池进行更换。

电池含锂，如果使用、操作或处理不当会发生爆炸。

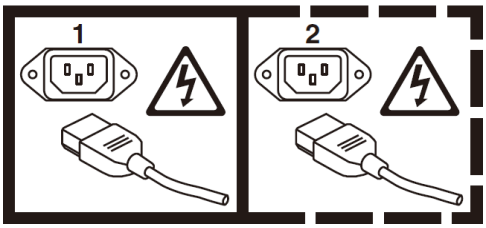
请勿：

- 将电池投入或浸入水中
- 将电池加热至超过 100°C (212°F)
- 修理或拆开电池

请根据当地法令法规的要求处理电池。

三、 注意：

设备上的电源控制按钮和电源上的电源开关并不切断提供给设备的电流。设备也可能有多根电源线。要使设备彻底断电，请确保断开所有电源线的连接。



四、 注意

切勿卸下电源外盖或贴有危险标签的任何部件的外盖。

五、 注意

此产品满足电磁兼容 A 级，在生活环境中，该产品可能会造成无线电骚扰。在这种情况下，可能需要用户对其骚扰采取切实可行的措施。

4 设备安装

4.1 SIVS708

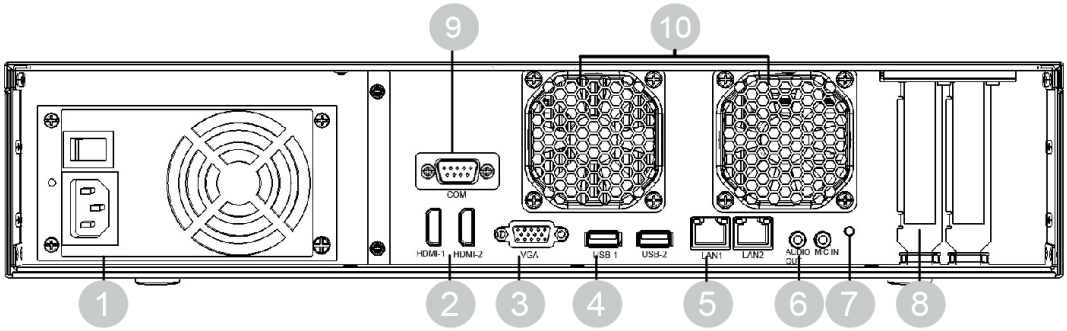
4.1.1 设备正视图

1、前置 USB2.0 接口 x2	2、前面板硬盘罩钥匙孔
3、设备状态指示灯（报警、运行、网络 1、网络 2）	4、设备开关
5、硬盘指示灯（HDD1-HDD8）	

4.1.2 前面板 LED 指示灯和按键

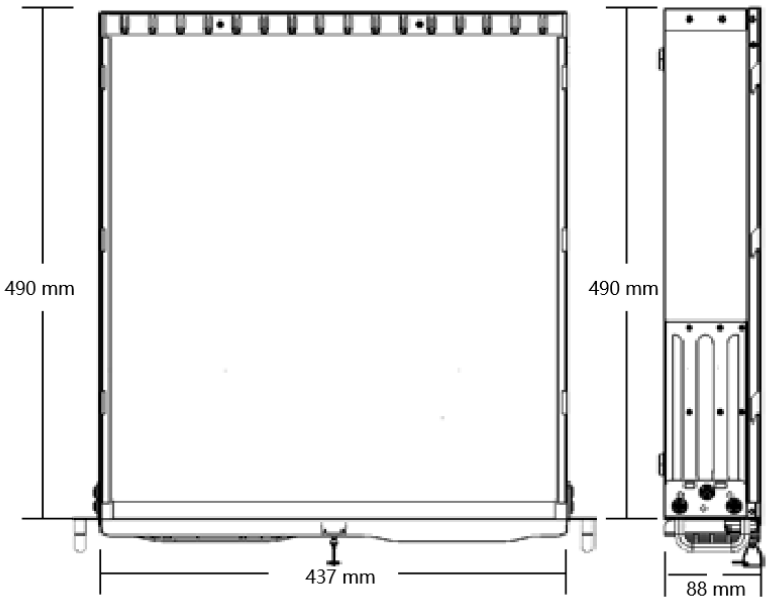
灯的丝印	灯名称	描述
ALARM	报警指示灯	通过硬件管理 API 资源实现此报警灯显示
RUN	运行指示灯	开机后此灯为蓝色长亮状态，关机，灯熄灭
LAN1、LAN2	网络指示灯 1、2	开机检测到网络连接时，灯亮；网络有数据传输时，此灯为蓝色闪烁状态；关机或开机没有连接网络时，灯不亮
⏻	设备按键开关（电源指示灯）	设备开机后，PWR 为蓝色长亮状态，断电灯熄灭，待机时亮红灯
HDD1-HDD8	硬盘指示灯	硬盘正常上电后，此灯为蓝色长亮；关机或开机没有检测到硬盘时，此灯不亮，硬盘报警时，红色常亮

4.1.3 产品后视图

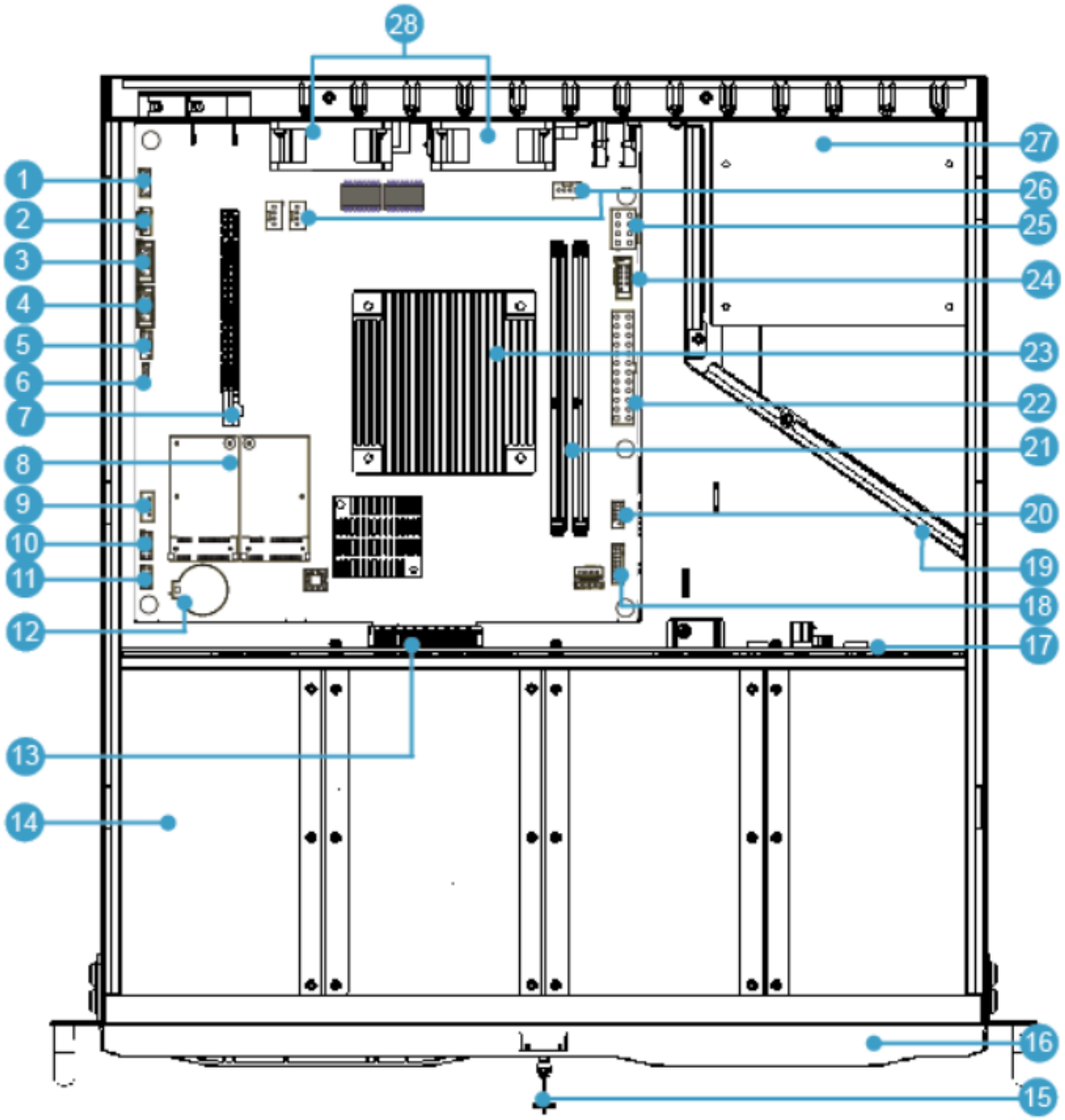


1、电源	2、HDMI 接口（1-2）	3、VGA
4、USB 接口（1-2）	5、RJ45 千兆网口（LAN1-LAN2）	6、AUDIO OUT/MIC IN 接口
7、重置按键	8、扩展槽挡片	9、COM 接口
10、机箱散热风扇		

4.1.4 设备外形尺寸



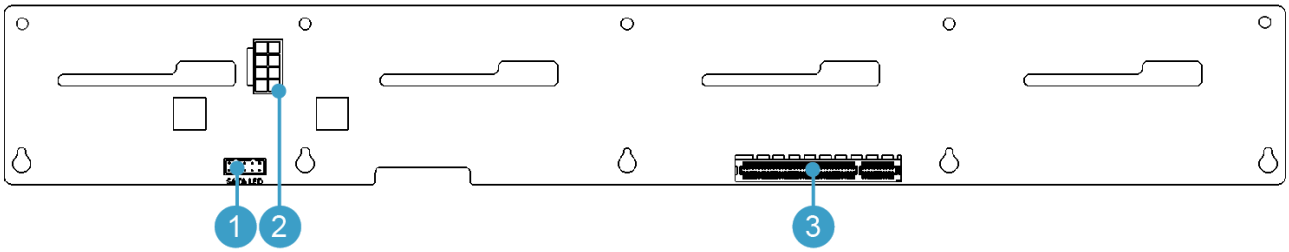
4.1.5 机箱内部结构



1、F_AUDIO	2、CD_IN	3、JCOM 3	4、JCOM4
5、FUSB6_7	6、JSPK	7、PCI-E8X_1	8、2x 电子盘（mSATA 接口）
9、USB2.0 接口	10、GPIO	11、FUSB1	12、系统电池
13、GOLD Finger（to SATA Backplane）	14、8*3.5 寸硬盘	15、前面板锁	16、可翻盖前面板
17、背板	18、JFP	19、电源隔风板	20、FUSB8_9
21、DIMM(1-2)	22、24Pin PWR	23、CPU	24、JCOM1_2
25、8Pin PWR	26、CFAN	27、电源	28、机箱散热风扇

4.1.6 背板快速参考

背板 A 面



1、SATA LED　2、背板电源连接器 3、背板与主板信号连接器

4.1.7 SATA 设备顺序

从产品正面看顺序编号，此 SATA 序号与前面板状态灯相对应：

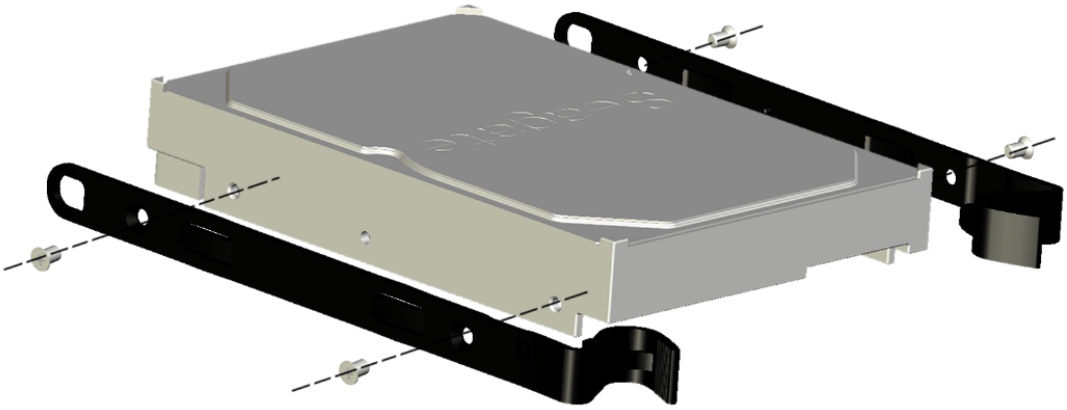
注：SATA 控制器在操作系统下获取的磁盘顺序和背板丝印有可能不一致。

4.1.8 热插拔 SATA 硬盘驱动器选件

说明：本节提供关于安装硬盘驱动器的操作说明。该设备可安装 1—8 块热插拔 SATA 硬盘。

安装步骤

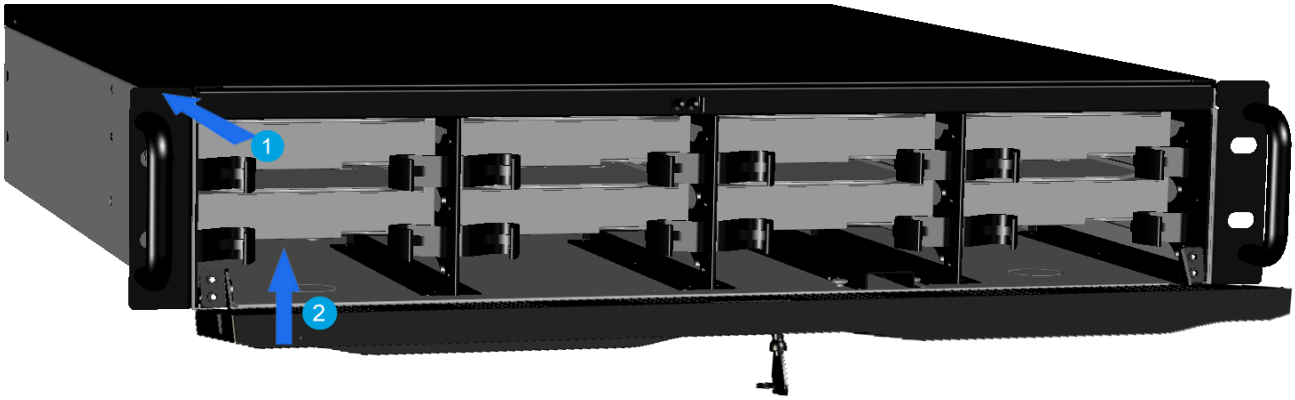
第一步：拿出配件盒中的硬盘 Tray，固定硬盘两侧螺钉，如下图所示：



第二步：拿出设备，使用配件盒中的设备前面板钥匙将前面板打开。

第三步 :将安装好 Tray 的硬盘驱动器依次推入设备插槽中 ,压入直至将其卡入到位(有明显的

“咔”声后），关上设备前面板，如下图 1、2 步操作：



说明：设备上电后，前面板硬盘指示灯没有变成蓝色，请检查硬盘驱动器是否安装到位，并处于良好状态。如果硬盘驱动器没有安装到位，前面板上的硬盘指示灯不亮。

4.2 SIVS724

4.2.1 设备视图

设备前视图：

图 1

注：机箱尺寸 625*482.6*177mm(长*宽*高)，4U 设备。

硬盘状态灯区

LED灯状态	说明
没有亮灯	没有磁盘
蓝灯恒亮	空闲磁盘
蓝灯恒亮，绿灯快闪	磁盘正在进行IO读写
蓝灯恒亮，绿灯恒亮	热备盘
蓝灯恒亮，红绿灯交错慢闪	磁盘物理定位中
蓝灯恒亮，红绿灯交错快闪	未激活磁盘
蓝灯恒亮，红灯恒亮	故障磁盘

图 2

如果插盘信号灯不亮，请检查：

1. 硬盘位置是否插到位。
2. 硬盘是否损坏。

设备后视图：

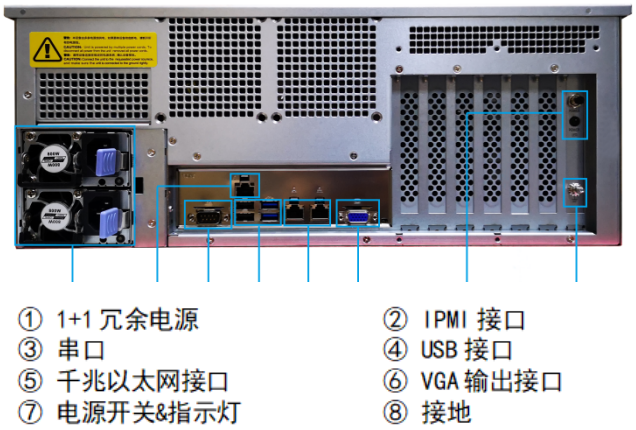


图 3

注：后视图，⑤左边是网卡 1，右边是网卡 2。

4.2.2 设备上架安装

描述：

使用机柜托盘进行安装。

注：安装时，应注意以下要求：

至少需要两个人才能将 SIVS 安全地提起并安装到机架中；

安装时请按规定佩戴防静电手套或防静电手环；

请勿在没有托盘支撑的情况下将 SIVS 安装到机架中；

安装 SIVS 或更换组件前，应确保所有开关及电源均已关闭；

建议 SIVS 上架前先不要安装磁盘，否则设备将非常重，容易造成重心不稳摔坏设备。

SIVS 安装时需要接地。

安装示意图：

上机柜托架

在 SIVS 上架之前把机柜托架装到大机柜中，安装螺母，如下图 4。

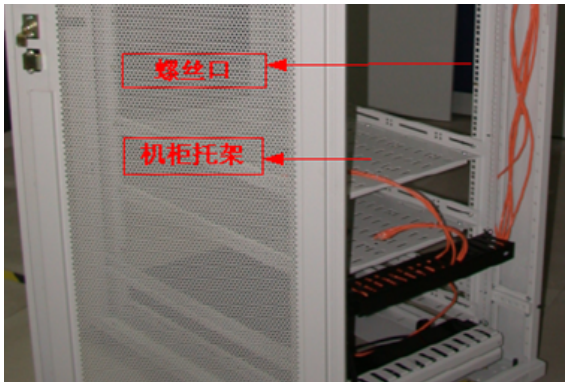


图 4

设备上架

图 5

注：机柜内设备间应留 1U 的空间，并固定设备与机柜间螺丝，保障 SIVS 的稳定运行。

4.2.3 安装硬盘

注：安装磁盘时要非常小心，磁盘非常脆弱，如掉到坚硬的平面（即使很低的高度），或者工具碰到磁盘上的回路都有可能损坏磁盘；安装磁盘时，遵守所有的防静电防护要求；使用配套的螺栓安装磁盘，更长的螺栓可能损坏磁盘；为获得最佳性能，请安装同型号同批

次磁盘。

盘位编号：

盘位编号，从左往右，从下往上编号。如 24 盘位设备：即左下角为盘位 1，右上角为盘位 24。如下图 6。

图 6

安装步骤：

1、从 SIVS 上取下硬盘托架；

2、小心地将磁盘驱动器放入磁盘托架的前部，使底部的螺钉孔和托架对齐。如图 7 所示。

3、将螺钉穿过磁盘托架的固定孔，然后拧入磁盘驱动器底部的固定孔，如图 8 所示。

4、将磁盘托架重新插入原槽位中，然后轻轻向里推。

5、关闭磁盘托架前的护盖。

6、磁盘托架插入后，SIVS 将自动扫描并识别磁盘。

7、重复以上步骤安装其它需要安装的磁盘驱动器。

图 7

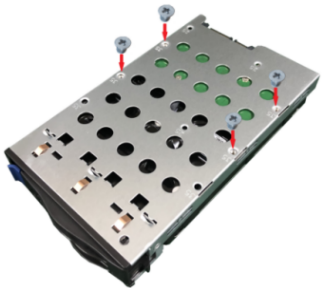


图 8

在使用 SIVS 前，需首先配置 SIVS 的 RAID 部分。

4.2.4 磁盘管理（RAID）界面

进入 SIVS 的磁盘管理界面。

把 SIVS 通过网线接入现有的网络中，可通过现有网络中的任意一台支持 WEB 浏览器的 PC 机来进行配置和管理存储管理系统。（浏览器使用 360 极速浏览器（极速模式））URL 地址栏中输入 SIVS 的默认磁盘管理界 IP 地址 :端口 8080(IP1 :https://100.0.0.1:8080 ,IP2：https://10.0.0.1:8080）并按回车键，如下图 9。

图 9

注：SIVS 出厂缺省网口 1：100.0.0.1/255.255.255.0

SIVS 出厂缺省网口 2：10.0.0.1/255.255.255.0

磁盘管理界面 https://默认 IP 地址：端口 8080（IP1：https://100.0.0.1:8080，IP2：https://10.0.0.1:8080）

在用户名编辑框内输入管理员用户（admin），在密码框中输入管理员密码（初始密码为 12345678），输入完毕点击登录按钮，进入存储管理系统。

4.2.5 创建 RAID

点击磁盘管理→RAID 管理选项，界面如下：

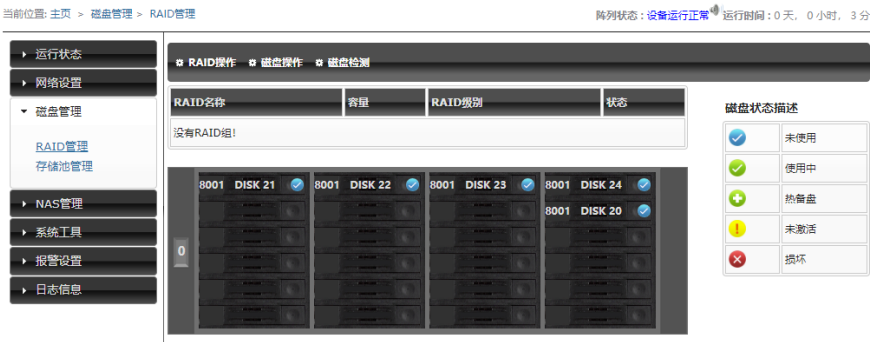


图 10

点击 RAID 操作，选择创建 RAID 选项，选择磁盘，设置 RAID 级别，块大小根据实际应用选择，容量不填。点击创建按钮。

图 11

注：RAID 组仅支持同类型磁盘创建 RAID！

注：RAID 级别建议使用 RAID 5；块大小建议使用 256KiB。

注：设置好 RAID 后，最多可以热插拔一块硬盘，切记不可热插拔多块硬盘，以免 RAID 散列造成数据丢失。关于 RAID 的使用，请自行查阅 RAID 的详细介绍。

界面上将显示 RAID 同步，在状态中看到初始化 RAID。

图 12

4.2.6 设置热备盘

点击磁盘操作→设置热备盘：

图 13

进入设置热备盘窗口：

图 14

选择做热备盘的硬盘，热备盘所属 RAID 组，点击设置，返回结果，如下图 15。

图 15

- **激活磁盘**

如果是使用过的磁盘并非空盘，且带有数据信息，则会显示黄色标识，需要清除磁盘信息。

点击磁盘操作→激活磁盘操作界面。

注：激活磁盘是不可逆的操作。

- **激活 RAID**

当 RAID 组处于失效或磁盘大部分显示黄色标识，可以使用激活 RAID 选项进行强制激活。

删除热备及 RAID 组

点击 RAID 操作→删除 RAID 及磁盘操作→删除热备盘选项。

4.2.7 创建 NASLUN

1、创建存储池

点击磁盘管理→存储池管理，点击创建存储池

图 16

点击确定，成功后如下图 17。

图 17

2、创建 NASLUN

点击磁盘管理→存储池管理→LUN，点击创建 NASLUN，在创建 NASLUN 对话框中点击下一步。

图 18

指定所需容量后，点击下一步。

图 19

3、创建映射

选择要映射的目录，可手动设置挂载点，点击下一步。

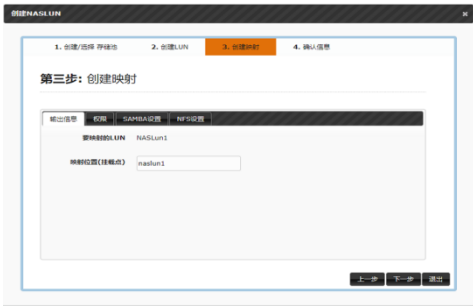


图 20

确认信息中可设置所需的文件系统格式，之后点击完成。

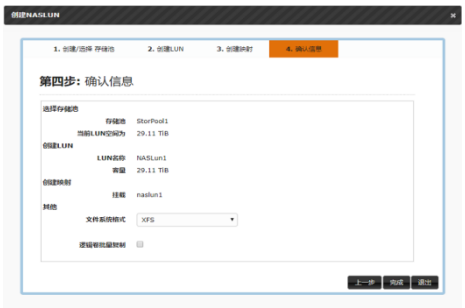


图 21

完成后，如下图 22。

图 22

注意：删除 RAID 后，需要先重启 SIVS 服务器后，才能重新创建 RAID，否则会重新 RAID 紊乱情况，导致录像存储错误。

注意 :需要先创建存储池 ,再创建 NASLUN。不创建存储池 ,直接创建 NASLUN 会出错。

5 环境要求及准备

5.1 空间要求与通风要求

为方便进行维修操作和正常通风 ,在决定机架的安装位置时请遵守以下空间和通风要求：

- 在机架前方至少留出 63.5 厘米（25 英寸）的空隙。
- 在机架后方至少留出 76.2 厘米（30 英寸）的空隙。
- 在两排机架的背面之间至少留出 121.9 厘米（48 英寸）的空隙。

服务器从前盖吸入凉风，从后盖排出热风。因此，机架的前后盖都必须通风良好，以使周围的空气进入机柜并将热气从机柜排出。

注意：为了避免散热不充分而损坏设备，请勿阻塞设备通风口，避免在粉尘较大的室内，避免安装在剧烈震动的场所。

5.2 温度要求

为确保设备能够持续安全可靠地运行，请将系统安装或放置在通风良好、温度可控制的环境中。

注意：为了减少温度对设备的危险，请注意以下事项：

不允许阻塞服务器周围的气流或使内部机架温度升高，以致超出最大允许限值。

5.3 电源要求

安装本设备时，必须遵守当地或区域有关安装信息技术设备的电气法规，而且必须由经过认可的电气工程师来完成安装操作。

警告：为减少人身伤害、火灾或设备损坏的危险，为机架供电的交流电源分支电

路不得超载。请向制定设备布线和安装要求的电气机构咨询。

注意：请使用调节式不间断电源（UPS），以免服务器受到电源波动和临时断电的影响。此设备可防止硬件因电涌和电压峰值的影响而受损，并且可在电源出现故障时使系统保持正常工作状态。

安装多台服务器时，可能需要使用其它配电设备来为所有设备安全供电。请遵守以下准则：

- 平衡可用交流电源分支电路之间的服务器电源负荷。
- 不允许系统总的交流电负荷超过分支电路交流电额定值的 80%。
- 请勿使用普通的电源接线板来连接本设备。
- 通过单独的电路为服务器供电。

5.4 电气接地要求

服务器机柜必须正确接地，以使其正常运行并确保安全。

5.5 机架/柜警告及要求

在机柜中安装服务器之前，请阅读以下准则：

- 在机架式机柜中安装该设备，需要两位或更多的安装人员。
- 确保服务器安装环境温度 0℃—50℃。
- 请勿阻塞任何通风孔，通常 15 厘米（6 英寸）的空间就可以提供适当的空气流动。

- 在机架式机柜中，请务必在安装的服务器上部或者下部留有开放空间，并确保适当的空气流通。
- 服务器只能安装在门上带有孔的机架式机柜中。
- 规划从机架式机柜底部开始安装设备，从下至上进行安装。
- 将最重的设备安装在机架式机柜底部。
- 请勿同时将多个设备拉出机架式机柜。
- 为便于在安装过程中进行操作，请卸下机架门和侧面板。
- 将服务器连接到正确接地的插座。
- 在机架式机柜中安装多个设备时，采取预防措施以避免机架使电源插座过载。
- 设备装满硬盘后较重，也可以在机器固定在架上之后，再将固定好硬盘的托架插入设备的槽位中。
- 装满硬盘的设备避免剧烈震动，以免硬盘及设备的损伤。

在满足以下要求的机架中安装服务器：

– 前部安装凸缘和前门内侧间的最小距离为 70 毫米（2.76 英寸）。

– 后部安装凸缘和后门内侧间的最小距离为 157 毫米（6.18 英寸）。抬起设备时请使用安全的做法，如下图所示：

≥18 千克
（39.7 磅）

≥32 千克
（70.5 磅）

≥55 千克
（121.2 磅）

6 故障排除

6.1 预诊断步骤

警告：为了避免出现潜在的问题，在卸下、更换、重新安装或修改系统组件之前，一定要先阅读服务器文档中的警告和注意信息。

1. 查看重要安全信息。
2. 收集症状信息
3. 做好服务器诊断的准备工作

警告：只有经过公司培训的授权技术人员才可以尝试修理本设备。详细介绍的所有故障排除和修理步骤只是为了进行部件/模块级别的维修。由于各种板卡和部件极为复杂，因此任何人不得尝试进行组件级别的维修或对任何印刷线路板进行改动。维修不当可能会危及安全。

6.2 症状信息

在解决服务器问题之前，应收集以下信息：

●发生故障之前发生了什么情况？在执行哪些步骤后出现了问题？

●服务器发生故障前做过哪些改动？

●最近是否添加或删除了硬件或软件？如果是，是否记得在服务器设置实用程序中根据需要更改了相应设置？

●服务器出现问题症状有多长时间？

●如果问题随机出现，会持续多长时间？出现的频率如何？

6.3 做好服务器诊断的准备工作

1. 确保服务器所处的操作环境不仅供电充足，而且能够控制温度及湿度。

2. 记录系统显示的所有错误消息。

6.4 系统故障排除

注意：设备的维修只能由经过认证的维修技术人员进行。您只能根据产品说明文件的授权，或者在联机或电话服务和技术支持人员的指导下，进行故障排除和简单的维修。未经公司授权的维修所造成的损坏不在保修范围内。

6.4.1 系统启动失败故障排除

对于所有其他启动问题，请注意屏幕上显示的系统消息。

6.4.2 外部连接故障排除

对任何外部设备进行故障排除之前，请确保所有外部电缆均已牢固地连接至系统上的外部连接器。

6.4.3 USB 设备故障排除

按照以下步骤对 USB 键盘/鼠标进行故障排除。

从系统中暂时拆除键盘和鼠标电缆，然后再重新连接。

将键盘/鼠标连接至系统另一面的 USB 端口。

将此键盘/鼠标更换为其它可正常工作的键盘/鼠标。

如果问题没有解决，请重新启动系统。

6.4.4 串行 I/O 设备故障排除

关闭系统和所有已连接至串行端口的外围设备。

将串行接口电缆更换为可正常工作的电缆，并打开系统和串行设备。

如果问题得以解决，请使用已知正常的电缆更换接口电缆。

关闭系统和串行设备，将该设备更换为同类设备。

6.4.5 受损系统故障排除

关闭系统和连接的外围设备，并断开系统与电源插座的连接。

打开机箱盖。

确保已正确安装以下组件：

- 主机板/扩充卡提升板（如果存在）
- 电源模块
- 冷却风扇
- 处理器和散热片

- 内存模块
- 硬盘驱动器托盘
- 硬盘驱动器背板
- 确保所有电缆均已正确连接。
- 合上系统护盖。

6.4.6 系统电池故障排除

备注：如果长期（几个星期或几个月）关闭系统电源，则 NVRAM 可能会丢失系统配置信息。这种情况是由有故障的电池引起的。

更换系统电池，将系统重新连接至电源插座，并打开系统。

在系统设置程序中重新输入时间和日期。

备注：某些软件可能导致系统时间加快或减慢。如果除系统设置程序期间以外，系统似乎正常运行，则问题可能是由软件而不是由有故障的电池引起的。

6.4.7 电源设备故障排除

通过拆卸和重新安装的方法来重置电源设备。

备注: 安装完电源设备后，请等待几秒钟，以便系统识别电源设备并确定其是否可以正常工作。

6.4.8 冷却问题故障排除

请确保不存在以下情况：

- 设备护盖、冷却导流板、填充面板、内存模块挡片或背面填充挡片等部件是否有被卸下。
- 环境温度太高。
- 外部通风受阻。
- 冷却风扇被卸下或出现故障。

6.4.9 系统内存故障排除

- 如果系统无法操作，请关闭系统和连接的外围设备，并且拔下系统的电源线。等待至少 10 秒钟，然后将系统重新连接到电源。
- 打开系统和连接的外围设备，并留意屏幕上的信息。
- 如果需要开箱检查内存，请先关闭系统和连接的外围设备，并断开系统与电源插座的连接。
- 拆下机箱上盖固定螺钉，打开机箱上盖。
- 检查内存通道，确保内存填充无误。
- 在各自插槽中重置内存模块。
- 盖上机箱上盖。
- 进入系统设置程序并检查系统内存设置。
- 如果问题未解决，请继续执行下一步。

- 如果诊断检测程序或错误信息标明特定内存模块有故障，请使用已知正常的内存模块更换该模块。
- 要对未指定的故障内存模块进行故障排除，请用相同类型和容量的内存模块更换第一个 DIMM 插槽中的模块。
- 如果屏幕上显示错误信息，这可能表示安装的 DIMM 类型有问题、DIMM 未正确安装或 DIMM 有故障。按照屏幕上的说明解决问题。
- 在系统进行引导时，注意观察所有显示的错误信息。

6.4.10 处理器故障排除

- 关闭系统和连接的外围设备，并断开系统与电源插座的连接。
- 打开机箱上盖。
- 确保已正确安装了处理器和散热片。
- 盖上机箱上盖，运行相应的检测程序。

7 更换系统电池

警告：如果新电池安装不正确，可能会有爆炸的危险。请仅使用相同类型或制造商推荐的类型更换电池。请参阅安全信息以了解更多内容。

注意：维修只能由经过认证的维修技术人员进行。您只能根据产品说明文件的

授权，或者在联机或电话服务和支持小组指导下，进行故障排除和简单的维修。未经公司授权的维修所造成的损坏不在保修范围内。

电池部件说明

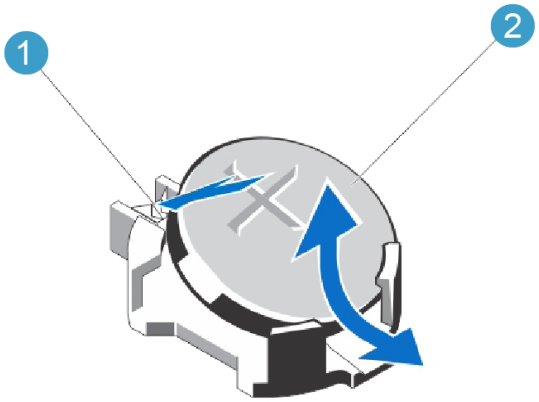


图 6-1：更换系统电池图

1、电池连接器的正极端

2、系统电池

==========

操作步骤

第一步：关闭系统，包括所有已连接的外围设备，并断开系统与电源插座和外围设备的连接。

第二步：拆下机箱上盖的 4 个固定螺丝，打开机箱上盖，找到电池插槽。

第三步：从连接器负极端的固定卡舌中取出电池。

第四步：要安装新的系统电池，通过稳固地向下按电池连接器的正极端来支撑电池连接器。拿住电池并使其“+”面朝上，将其滑入连接器正极端的固定卡舌下。

第五步：竖直向下将电池按入连接器，直至其卡入到位。

第六步：将系统重新连接至电源插座，并打开系统，包括所有连接的外围设备。

8 静电释放

8.1 防止静电释放

为避免损坏设备，在安装设备或取放部件时应注意采取必要的防范措施。手指或其它导体所释放的静电可能损坏主板或其它对静电敏感的设备。由静电造成的损坏会缩短上述设备的预期使用时间。

要避免静电损害，请注意以下事项：

- 将产品装入防静电包装中，以免在运输和存储过程中直接用手接触产品。
- 在将静电敏感部件运抵不受静电影响的工作区之前，请将它们放在各自的包装中进行保管。
- 先将部件放置在接地表面上，然后再将其从包装中取出。
- 请勿触摸插针、导线或电路。
- 在触摸静电敏感元件或装置时，一定要采取适当的接地措施。

8.2 防止静电危害的接地方法

接地的方法有几种。在取放或安装静电敏感部件时，您可以使用以下一种或多种接地方法：

- 您可以使用腕带，该腕带利用接地线与接地的工作区或计算机机箱相连。腕带必须能够灵活伸缩，而且内置安全电阻至少为 1 兆欧姆（±10%）。要达到接地目的，佩戴时请将腕带紧贴皮肤。
- 在立式工作区内，请使用脚跟带、脚趾带或靴带。当您站在导电地板或耗散静电的地板垫上时，请在双脚上系上带子。
- 请使用导电的现场维修工具。
- 配合使用耗散静电的折叠工具垫和便携式现场维修工具包。

如果您没有上述推荐使用的接地装置，请与授权经销商联系要求安装相应的装置。

如果需要详细地了解有关静电或产品安装的辅助信息，请与授权经销商联系。

9 SIVS 登录

登录 SIVS 基于 360 极速浏览器（极速模式），登录时使用 PC 打开 360 极速浏览器，主要有密码登录和 USBkey 登录两种登录方式，下面会逐一举例说明。

9.1 控件安装和卸载

首次使用 SIVS 时，打开 360 极速浏览器（极速模式），在浏览器中输入 SIVS 的默认地址 URL 例如：

SIVS708 出厂 http://192.168.1.101

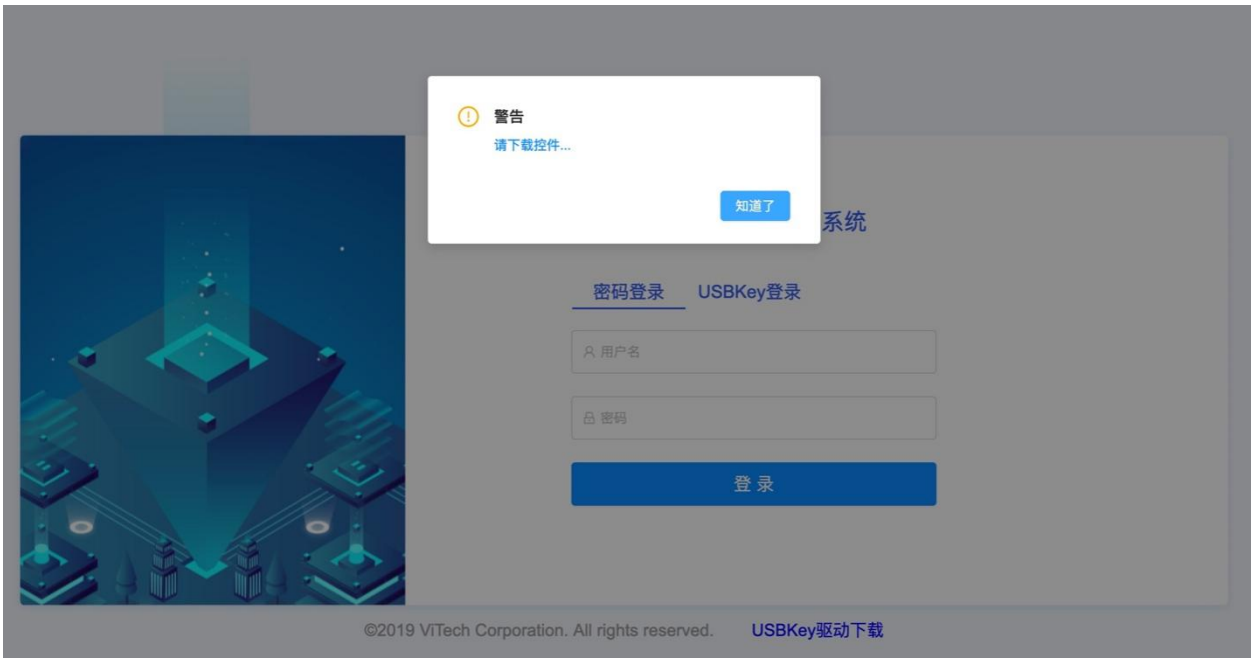
SIVS724 出厂网口 1:http://100.0.0.1　　网口 2:http://10.0.0.1

回车，打开 SIVS 的登录界面。

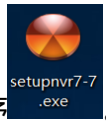
注：输入的地址是：http://192.168.1.101，不是：https://192.168.1.101

9.1.1 控件安装

初次登录时界面会提示安装控件，点击“请下载控件”：



注：安装时请关闭浏览器

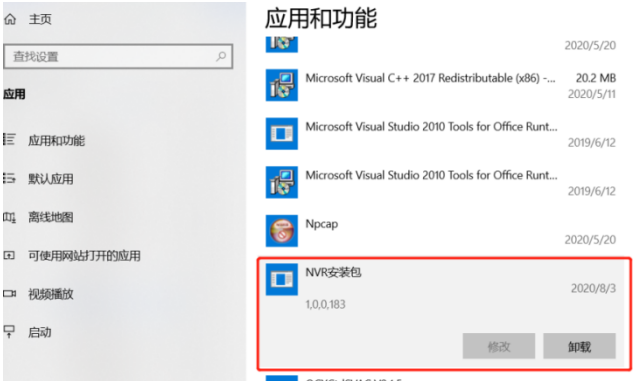
打开控件安装程序 

。直接按提示，点击下一步：

点击“完成”，完成插件的安装。

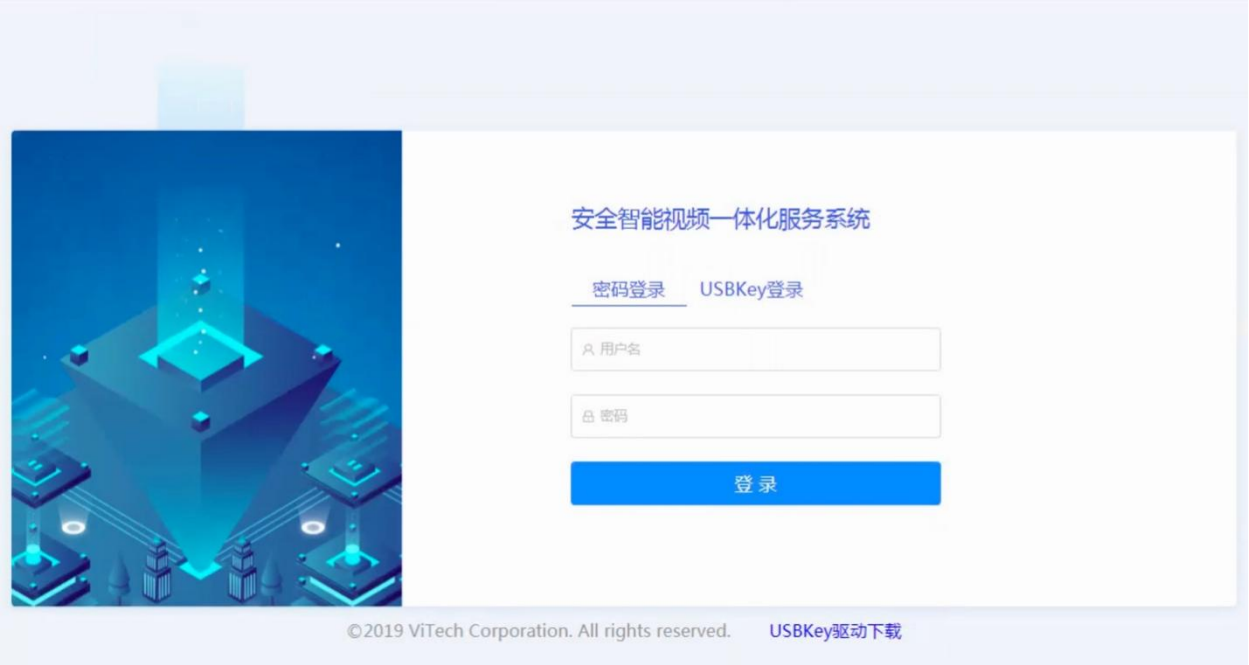
9.1.2 控件卸载

打开控制面板，点击“应用和功能”，找到“SIVS 安装包”，点击“卸载”，即可卸载 SIVS 的控件。



9.2 密码登录

选择“密码登录”，输入用户名和密码进行登录。SIVS 默认用户名：admin，默认密码：admin。



9.3 USBkey 登录

登录界面选择 USBkey 登录，下拉列表选择 PC 插入的 USBkey，点击登录。

输入 USBkey 的 PIN 码。（默认 PIN 码 88888888。）

注：使用 USBkey 前，要在 PC 上安装 USBkey 的驱动。点击“USBkey 驱动下载”，如下图。

下载安装完成后，即可在 USBkey 登录下拉列表中显示此 USBkey 的国标编号。如下图。

注：请使用中星微公司提供的 USBkey，USBkey 使用前需要提前发好证书。请与技术人员核实 USBkey 证书的获取途径。

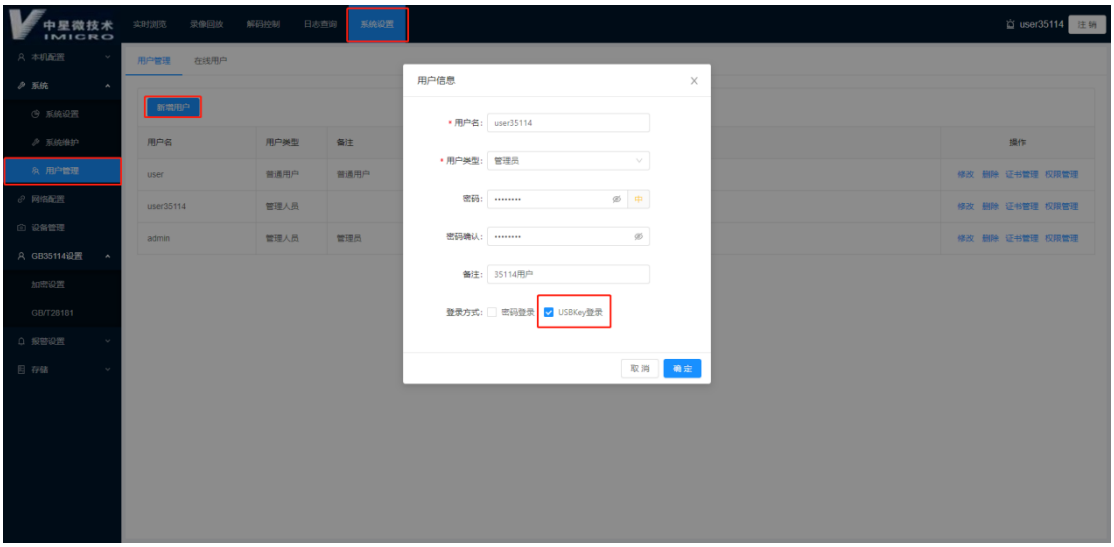
注：SIVS708 出厂随机附带一个用户 USBkey，已经预发了中星微技术的证书，证书导出请参考“附录四 USBkey 证书的验证及导出”。如果需要指定 CA 证书或另购的 USBkey

未发证，请参考“附录三 用户 USBkey 证书的导入”。SIVS724 出厂不附带用户 USBkey，需要额外采购。

注：SIVS 默认不使用 USBkey 登录，需要提前进行设置，并给新建用户设置权限。

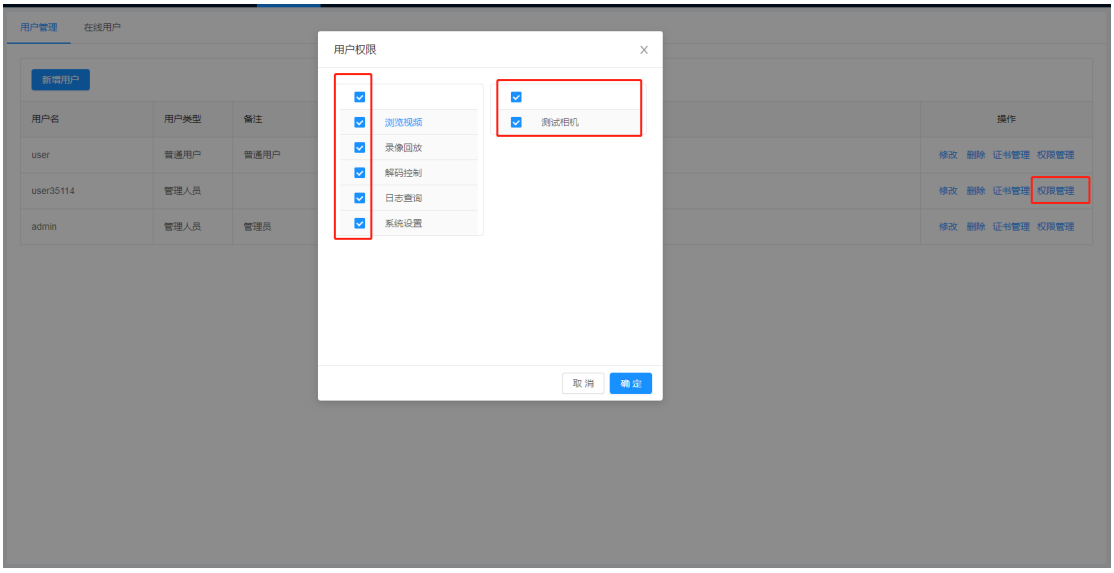
操作方法：

1、用户设置使用 USBkey 登录。使用 admin 用户登录后，点击系统设置→系统→用户管理，进入用户管理界面，选择已有用户，点击“修改”（或新建用户），勾选“USBkey 登录”，点击确定。如下图。



2、点击用户的“证书管理”，上传 USBkey 的加密证书和签名证书，点击确定。如下图。

3、用户设置权限。如果是新建用户，需要给用户设置权限。点击系统设置→系统→用户管理，进入用户管理界面，选择需要设置权限的用户，点击其后的“权限管理”，打开权限设置对话框，勾选该用户所需权限。另，每项内容下有子内容，需要点开进行设置。例如：浏览权限，点击后，会打开子内容显示 SIVS 有多少相机，可以全选，也可以根据需要选择。点击确定，进行保存。如下图。



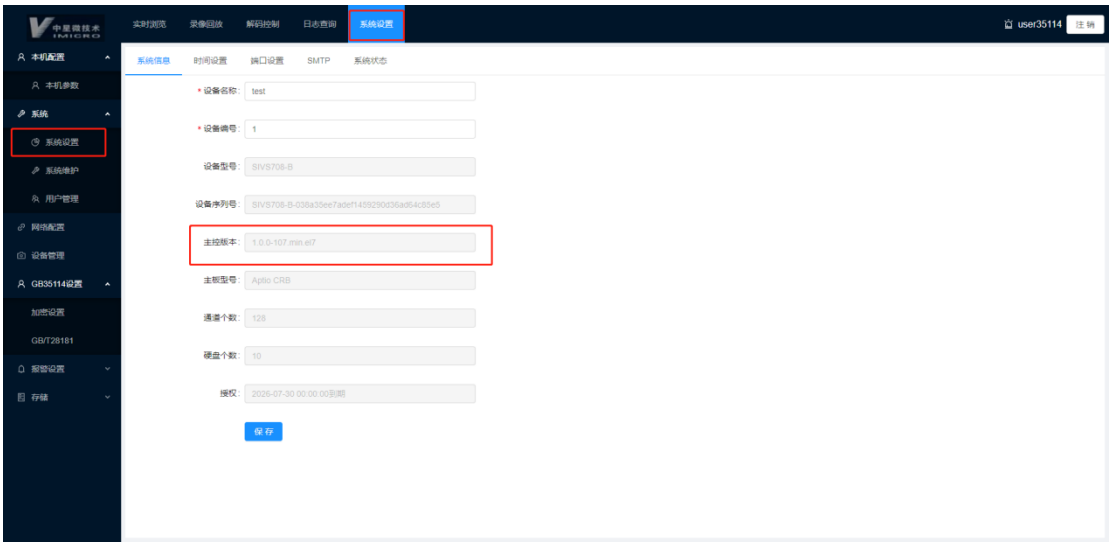
9.4 版本确认

登录 SIVS 后，首先进行版本确认，是否为最新版本。请将版本信息页面截图发给技术人员进行确认。如是最新版本，即可正常使用。如版本较旧，技术人员会发新版本，请使用新版本升级。

9.4.1 版本确认

操作方法：

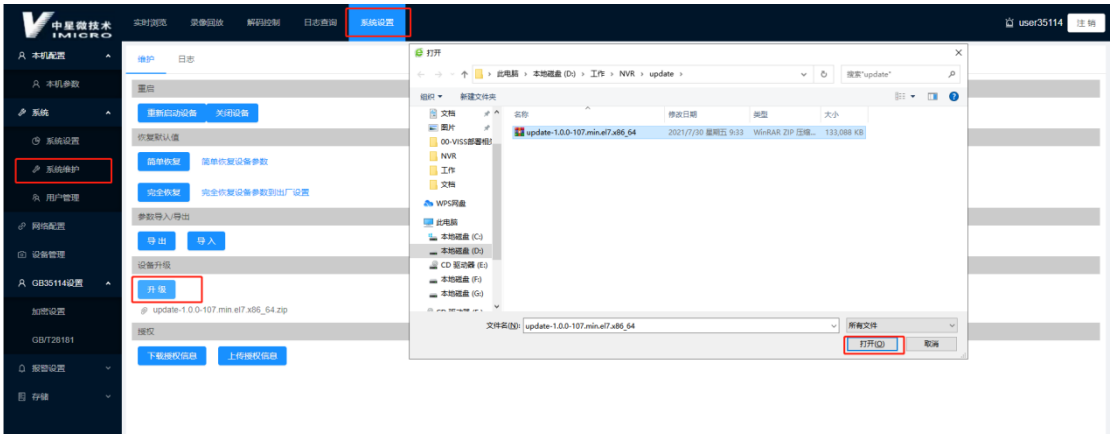
1、点击系统设置→系统→系统设置，进入系统信息界面，将此界面截图，发给技术人员。如下图。



9.4.2 版本升级

操作方法：

1、点击系统设置→系统→系统维护，进入系统维护界面，点击升级钮，选择新版本文件，即可进行升级。如下图。

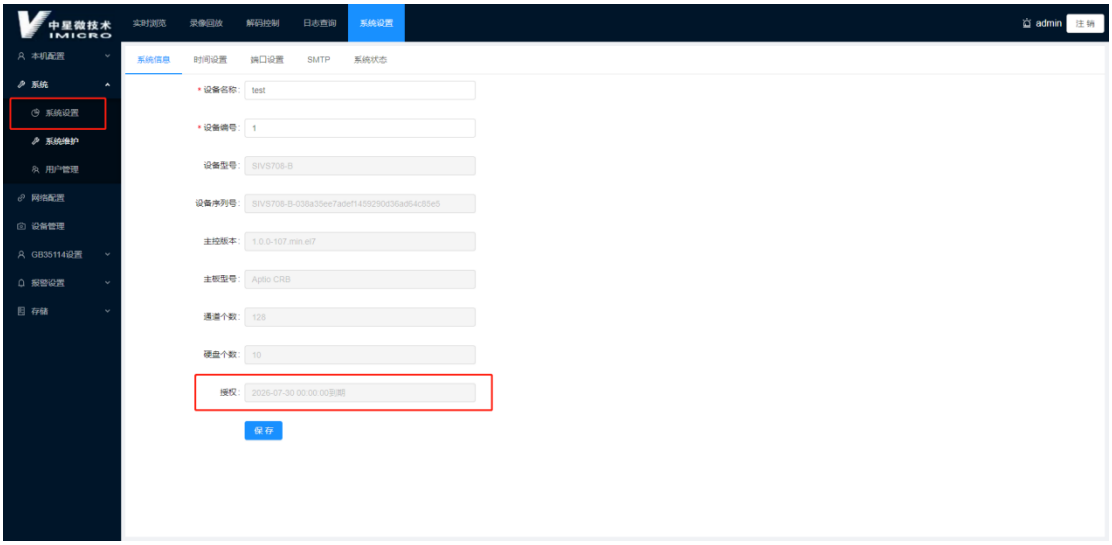


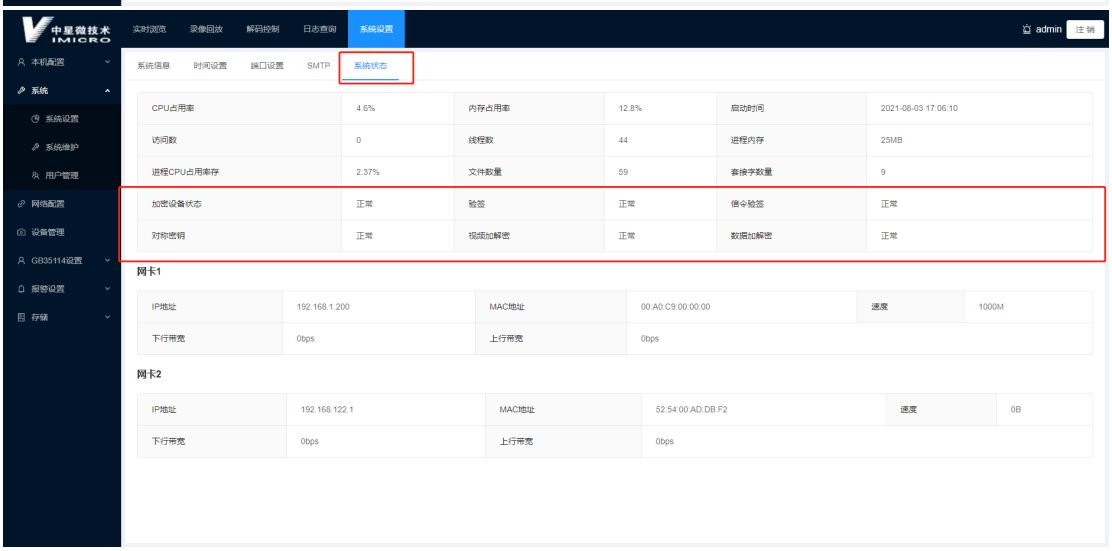
注：点击升级后，SIVS 会自动上传升级包进行升级。

9.5 检查系统状态及授权信息

点击系统设置→系统→系统设置，进入系统信息界面，检查授权是否正常。如因特殊情况显示“未授权”，请参考“SIVS 授权申请”章节。（出厂默认已授权）

进入系统状态界面，检查设备状态是否正常。

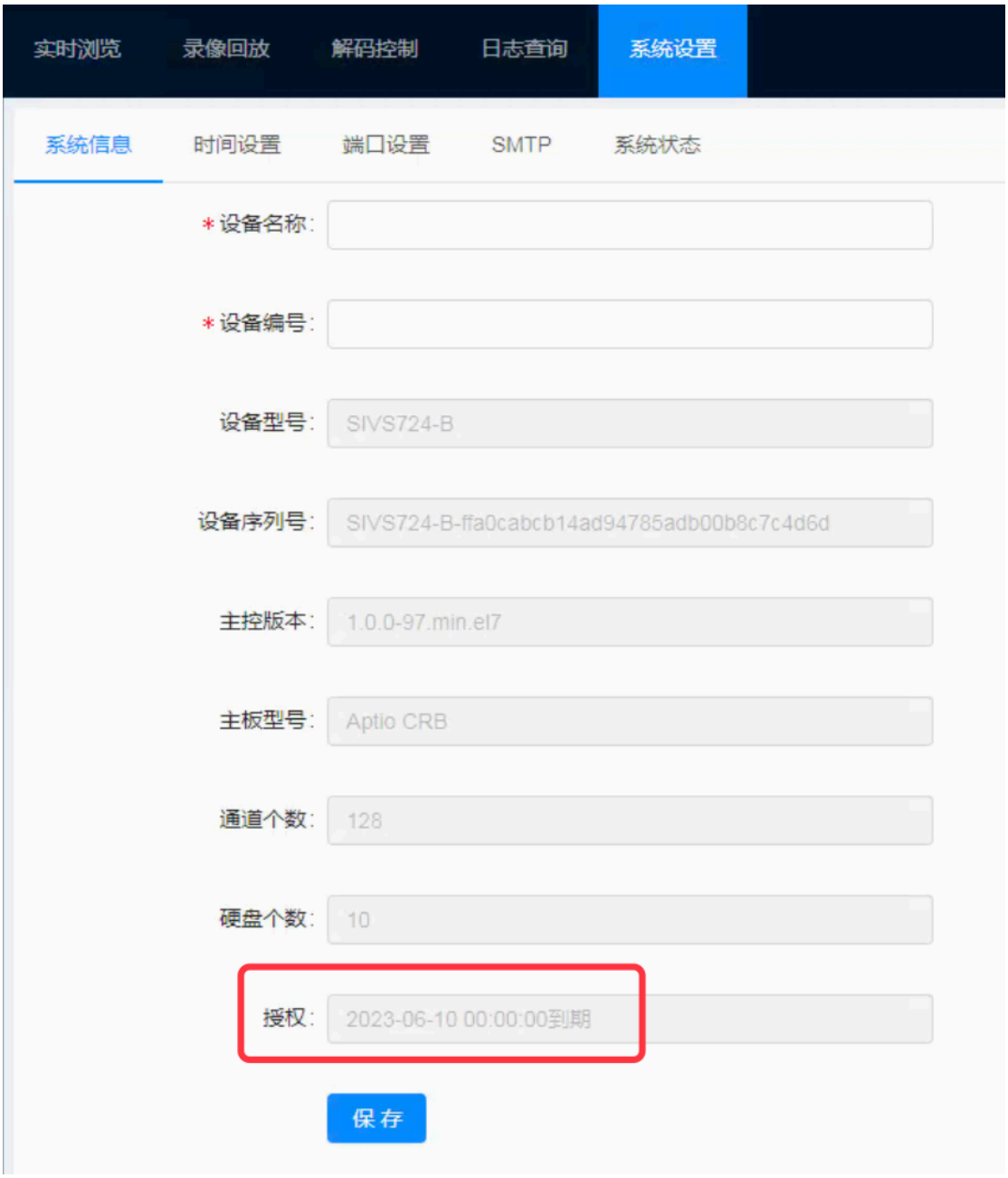




10 SIVS 授权申请

10.1 确认授权信息

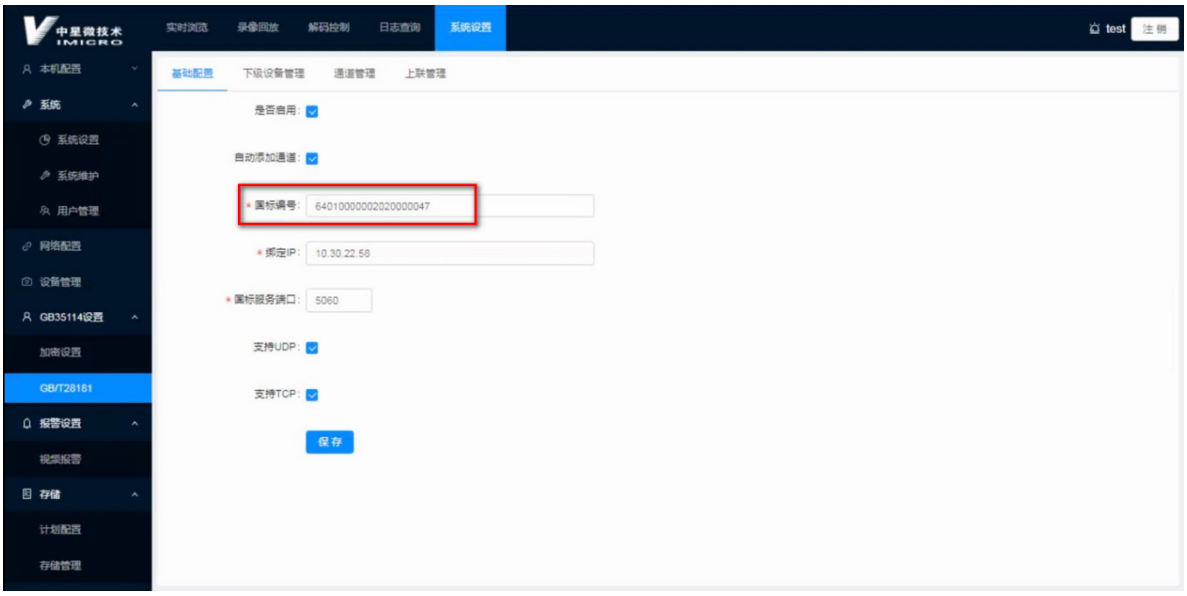
点击菜单“系统设置”，进入系统信息页面



确认授权信息，如果正确显示授权时间信息，请跳过此章节流程，如果显示“无授权”或者“授权已到期”，请继续该流程。

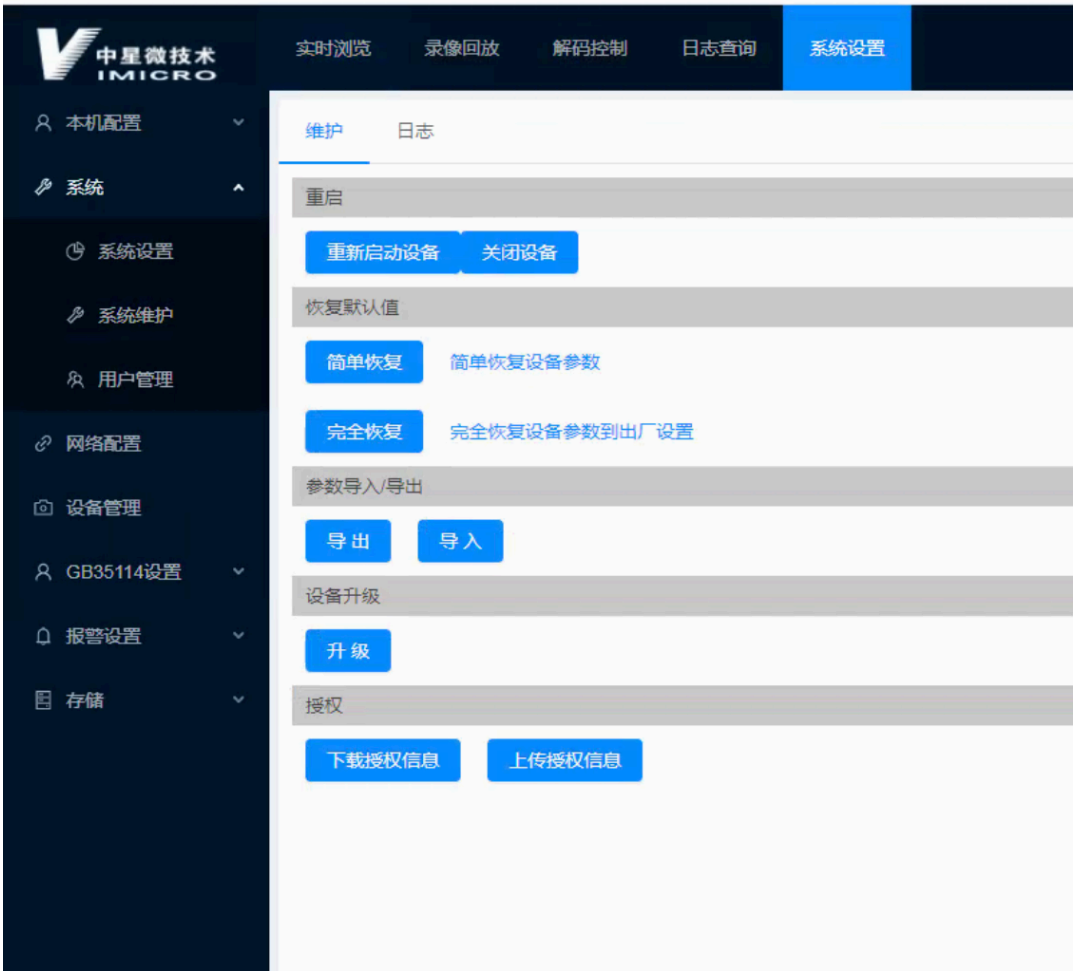
10.2 复制国标编号

双击设备国标编号，复制国标编号

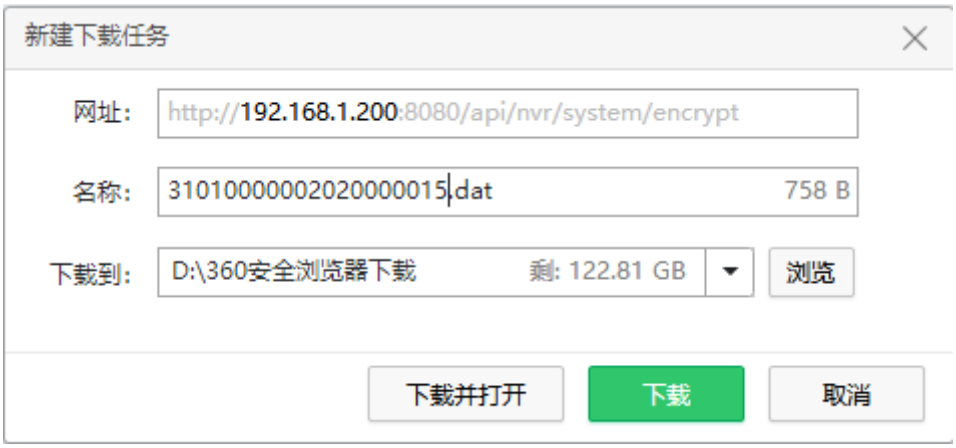


10.3 生成授权信息文件

点击系统设置-系统-系统维护



点击下载授权信息，将文件名字更改为刚才复制的国标编码



10.4 发送授权申请邮件

将下载完成的 XXX.DAT 授权文件发邮件至中星微技术

邮件格式如下：

邮件标题：安全智能视频一体化服务系统授权文件申请-(20xx-xx-xx)

邮件内容：

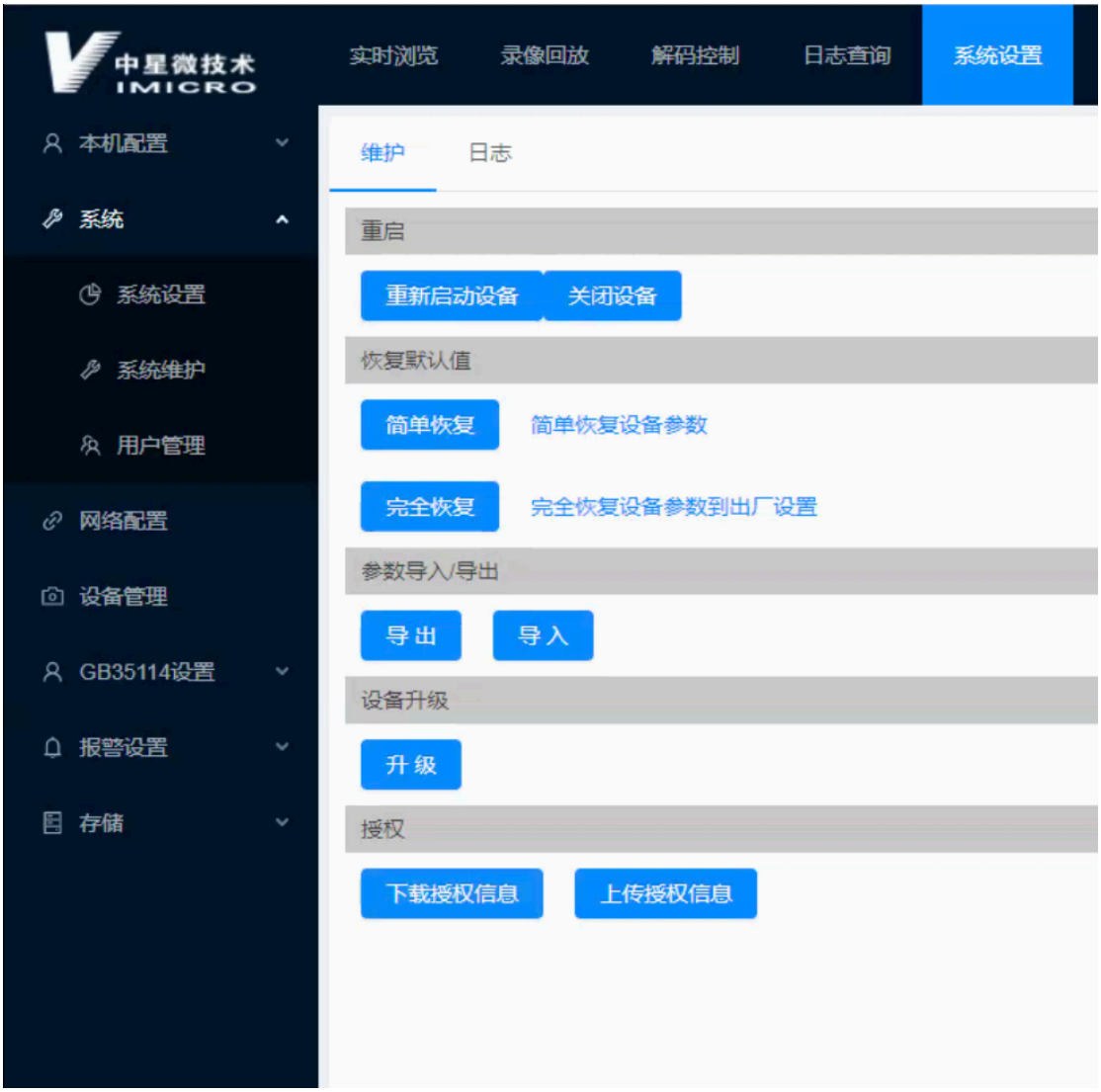
申请日期	项目名称	申请方	项目合同号	项目性质	主控版本	申请型号	联系方式
				临时/商用/ 重新申请			

附件附上更名后的授权文件（dat），如有多个授权申请，需将所有文件附上

10.5 授权文件上传

收到邮件发送的授权文件后，将文件上传至系统，文件格式为序列号.lic

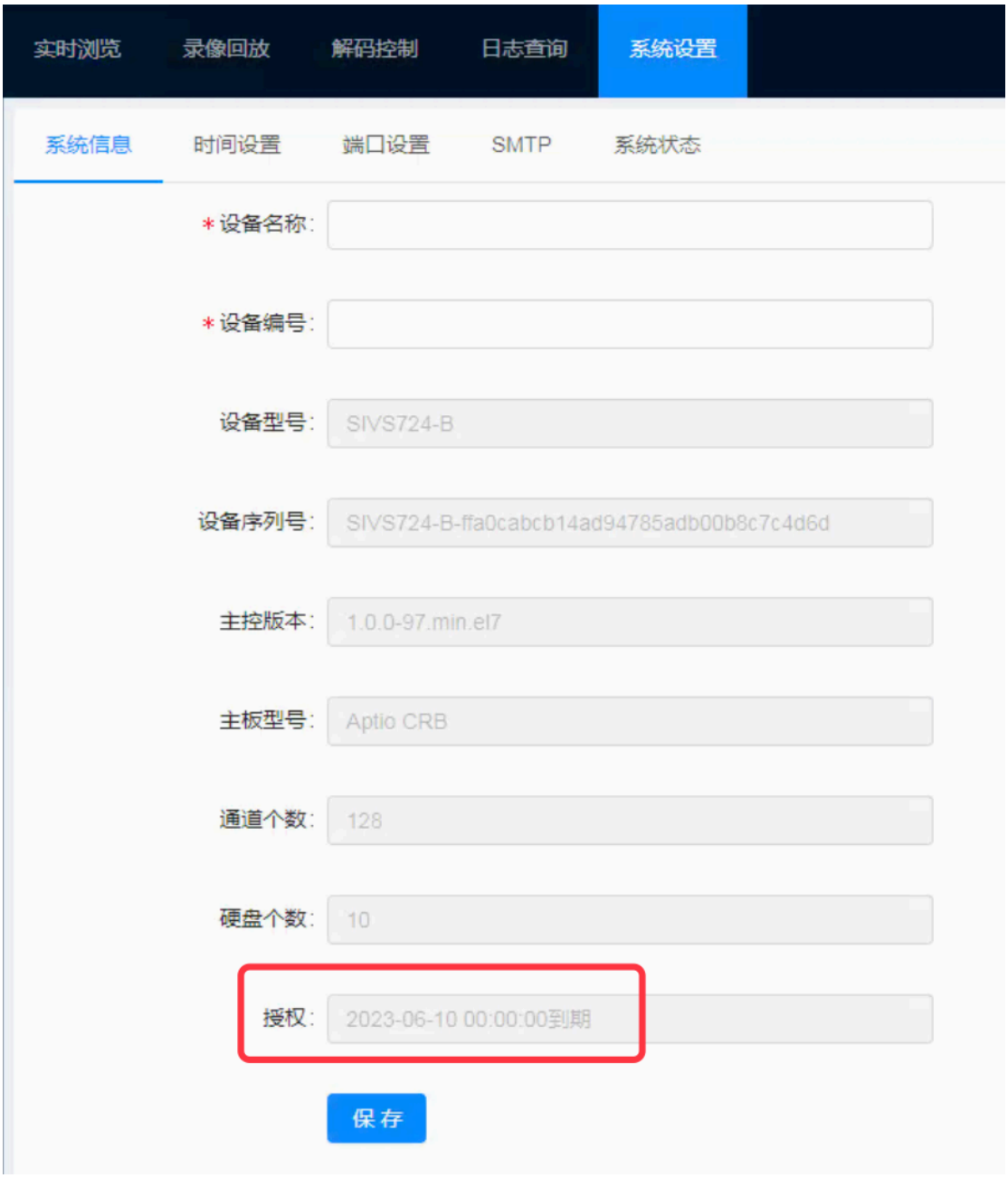
点击系统设置-系统-系统维护



点击“上传授权信息”，选择对应的 lic 文件，完成授权文件上传

10.6 确认授权信息

确认授权信息是否正确，点击菜单“系统设置”，进入系统信息页面



确认授权信息，如果显示“无授权”或者“授权已到期”，请与相关技术人员联系，如正确显示授权时间信息，则结束此流程。

注：授权与使用的密码产品绑定，使用过程中请先完成密码设备设置及发证工作。授权后，请勿随意更改密码设备，一旦更改，需尽快申请新授权。

11 SIVS 添加相机及其他配置

在本章节“GB35114 设置”子章节中讲述怎样添加相机。SIVS 所有的配置设定都使用密码登录来完成。

GB35114 安全功能基于 GB/T28181 协议实现，在进行 SIVS 配置前，请提前规划好：1）、SIVS 的 IP 等网络信息；2）、SIVS 的国标 ID；3）、相机的 IP 等网络信息；4）、相机的国标 ID；5）、使用 GB35114 安全功能的相机进行归类；6）、USBkey 的国标 ID；7）、相机的通道名称（如果是公安项目则还要提前规划地点标注）。

注：国标 ID 的规划，请严格按《GB/T 28181-2016 安全防范视频监控联网系统信息传输、交换、控制技术要求》进行规划。

可以参考本手册“附录六、国标 ID 简易介绍”。

注：国标 ID 不允许有重复。否则，证书有可能不能正常发放。

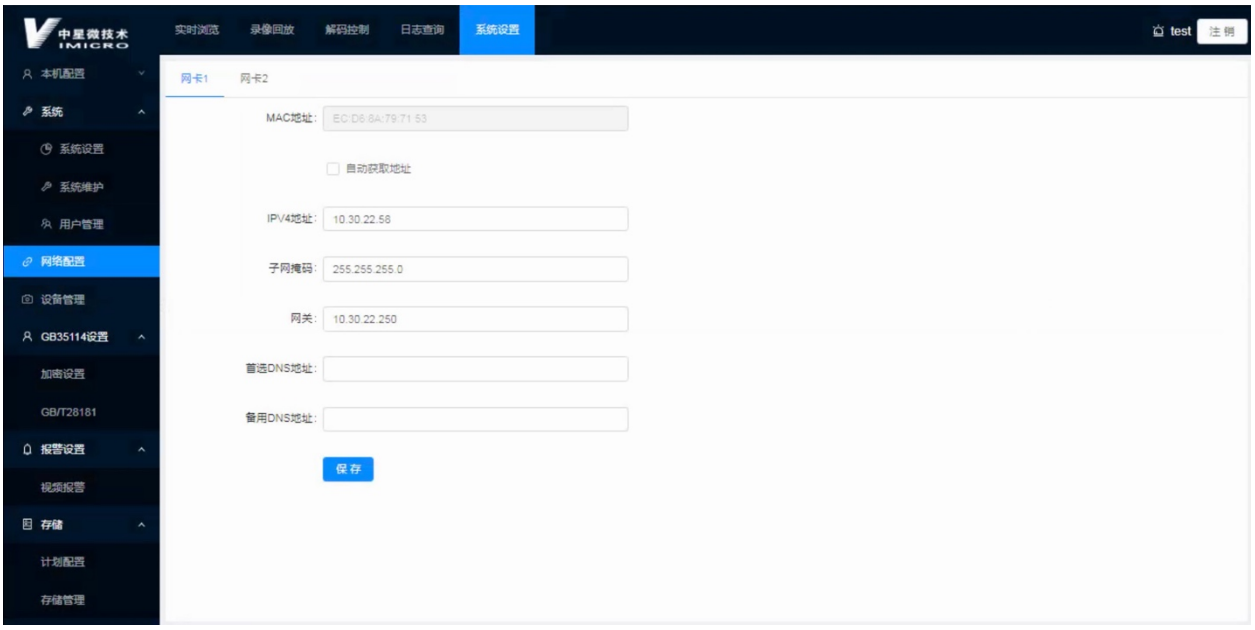
11.1 网络配置

进行 SIVS 网络配置，SIVS 自带两个网卡，网卡 1 和网卡 2。两个网卡都可以进行配置。具体内容根据设备需求进行设定。包括：IP、掩码、网关、DNS 等。

操作方法：

点击系统设置→网络配置，进入网卡 1 配置界面，输入相应的 IP、掩码、网关、DNS 等信息，点击保存。

网卡 2 配置方法相同。



注：不建议使用“自动获取地址”。

11.2 SIVS 国标 ID 等信息及证书

在进行添加相机前，需要获取 SIVS 的国标 ID 等信息及 SIVS 的证书，以便相机可以有配置信息。

11.2.1 SIVS 国标 ID 等信息的获取及修改

SIVS **国标 ID 等信息的获取及修改。**

操作方法：

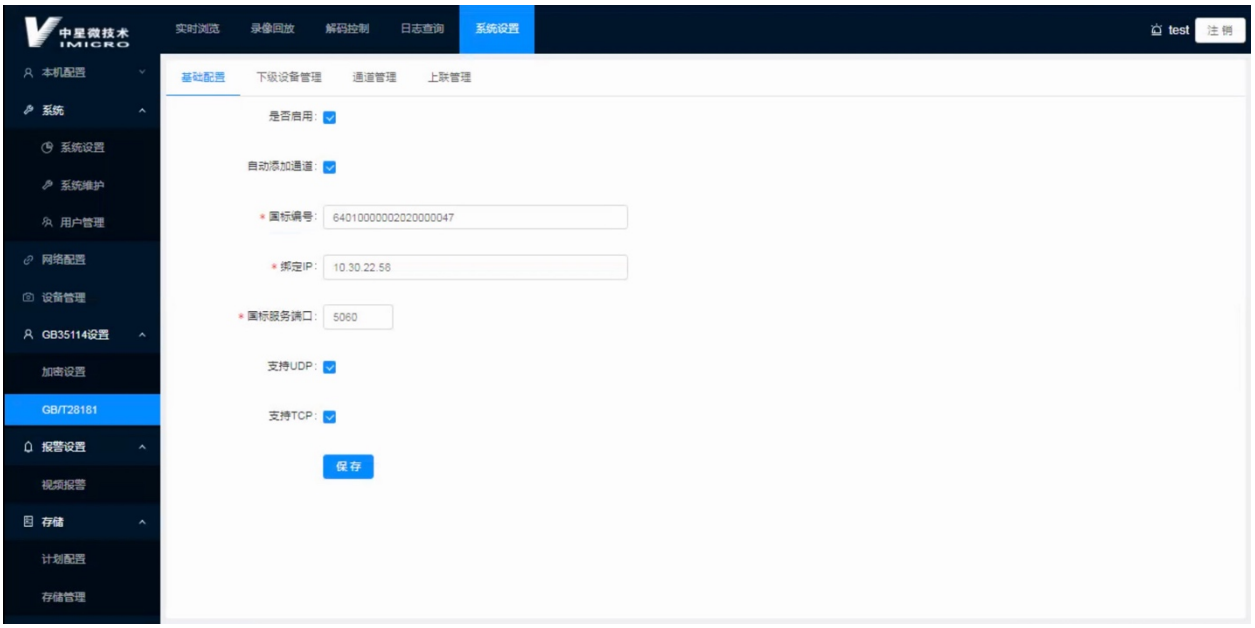
系统设置→GB35114 设置→GB/T28181→基础配置，此界面中：

1）、国标编号：即为 SIVS 国标 ID。

2）、绑定 IP：SIVS 的 IP 地址，填写相机需要注册的 IP 地址。SIVS 可以设置两个 IP 地址，需要相机注册网卡 1 的 IP 地址，此内容填写网卡 1 的 IP 地址；需要相机注册网卡 2 的 IP 地址，此内容填写网卡 2 的 IP 地址。

3）、国标服务端口：SIVS 作为上级的端口。即相机向 SIVS 注册时填写的 SIP 服务器端口。

4）、勾选“是否启用”、“自动添加通道”、“支持 UDP”、“支持 TCP”。



11.2.2 SIVS 证书的申请，获取及修改

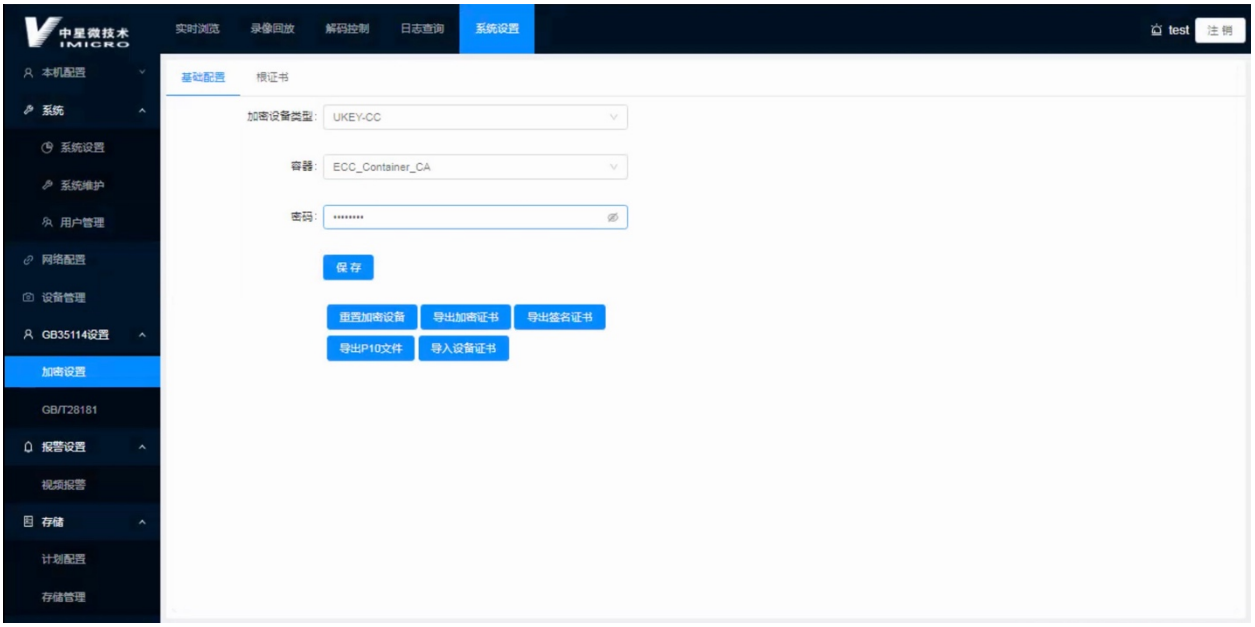
注：SIVS 设备 USBkey 或加密卡内置在主板里，出厂已经预发了中星微技术的证书，如果不需要指定 CA 证书，可跳过此章节。

1、使用 SIVS 配套 USBkey，生成 P10 文件，生成方式如下：

操作方法：

点击系统设置→GB35114 设置→加密设置→基础配置，点击导出 P10，弹出下载对话框，选择 PC 的文件夹进行保存，将保存的 P10 文件及 SIVS 的国标 ID 信息发给中星微技

术。拿到新证书后，点击导入设备证书，将新证书压缩包导入。对话框选择证书压缩包导入即可。

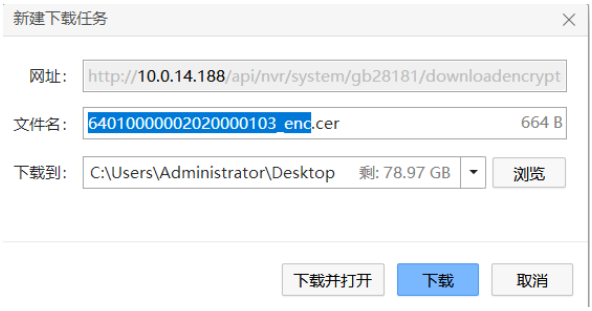


SIVS708 图

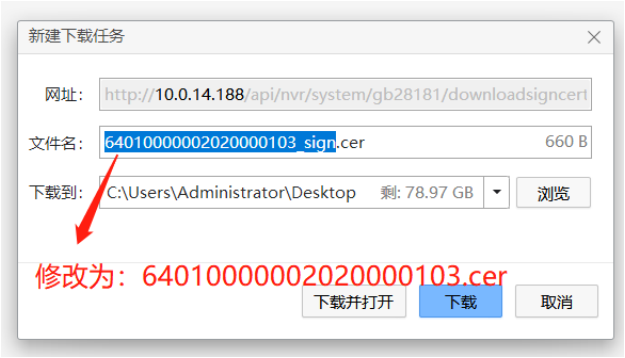
SIVS724 图

可以使用证书导出功能，导出加密及签名证书，操作如下：

1、点击系统设置→GB35114 设置→加密设置→基础配置，导出加密证书，直接按提示的文件名进行保存即可，见下图：



2、点击系统设置→GB35114 设置→加密设置→基础配置，导出签名证书，需要修改为“国标 ID.cer”，目的为相机对格式有要求。见下图：



注：修改国标 ID 后需要重新发放证书。获取方式同上。

11.3 GB35114 设置（添加相机）

SIVS 添加相机前或添加相机时，相机也需要进行配置。请参考“附录一、相机配置”和“附录二、相机证书的发放”。

SIVS 上添加相机，在“系统设置→GB35114 设置”中进行添加。

GB/T28181 协议相机和 GB35114 安全功能相机都使用此种方式添加。二者添加方式的区别：1、GB/T28181 协议相机不需要上传证书；2、认证方式不同，GB/T28181 协议相

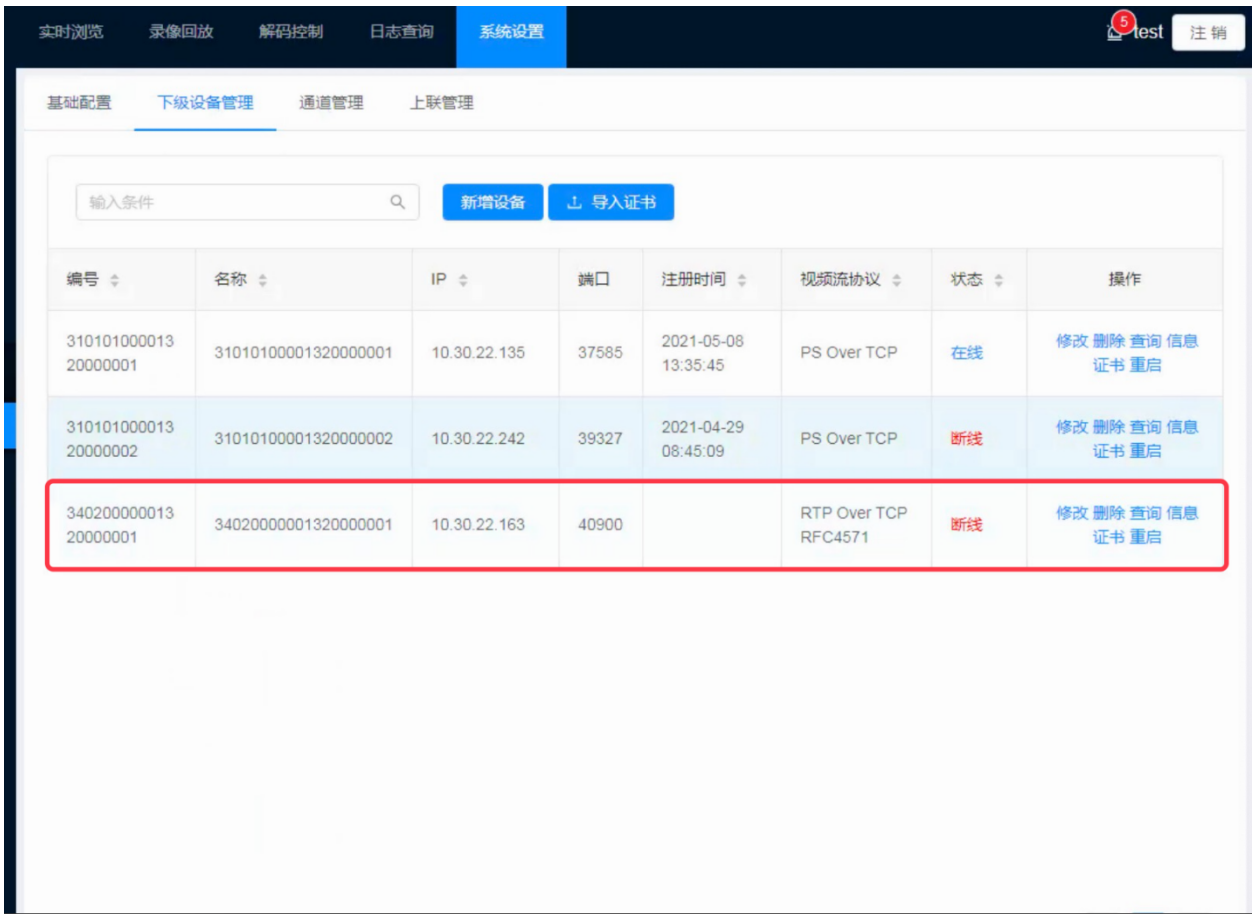
机选择“密码认证”，GB35114 安全功能相机，选择“数字证书双向认证”。具体操作如下：

11.3.1 系统自动添加相机

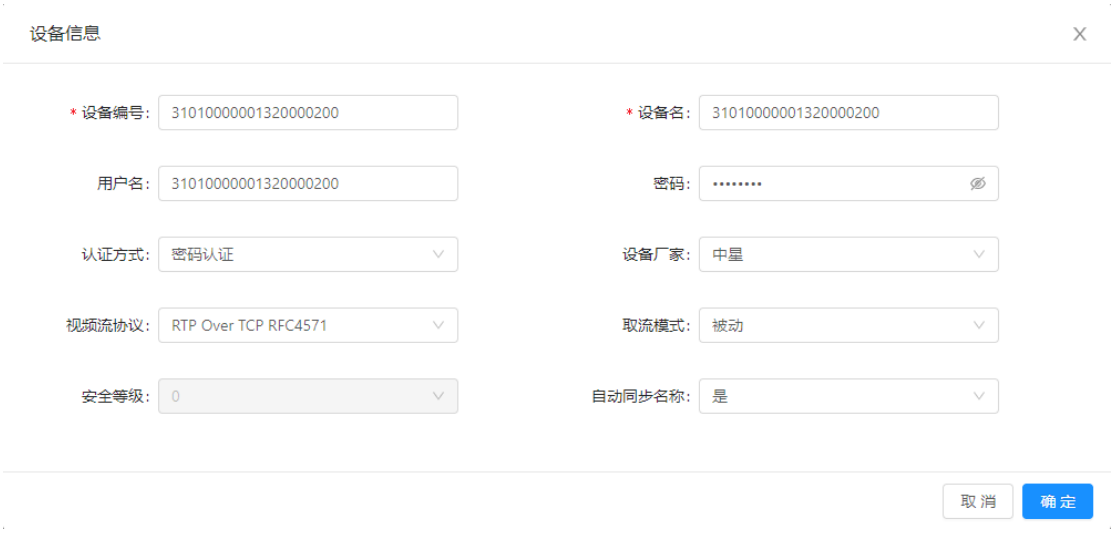
操作方法：

按照附录一和二的指导，完成相机配置，此时相机会主动向 SIVS 进行注册。

点击系统设置→GB35114 设置→GB/T28181→下级设备管理，找到自动注册的前端相机信息



点击修改



选择和填写以下相应内容：

1）、设备编号。填写相机的国标 ID。

2）、设备名。即相机的名称。

3）、用户名。需与相机国标对接配置中的设备号一致。

3）、密码。需与相机国标对接配置一致。默认：12345678。详见“附录一、相机配置”。

4）、认证方式。添加 GB/T28181 协议相机选择“密码认证”；添加 GB35114 安全功能相机，选择“数字证书双向认证”。

5）、设备厂家。选择“中星”，或按实际接入情况选择。

6）、视频流协议。选择“RTP Over TCP RFC4571”。

7）、取流模式。选择“被动”。

8）、自动同步名称。选择“否”。

点击确定进行保存。

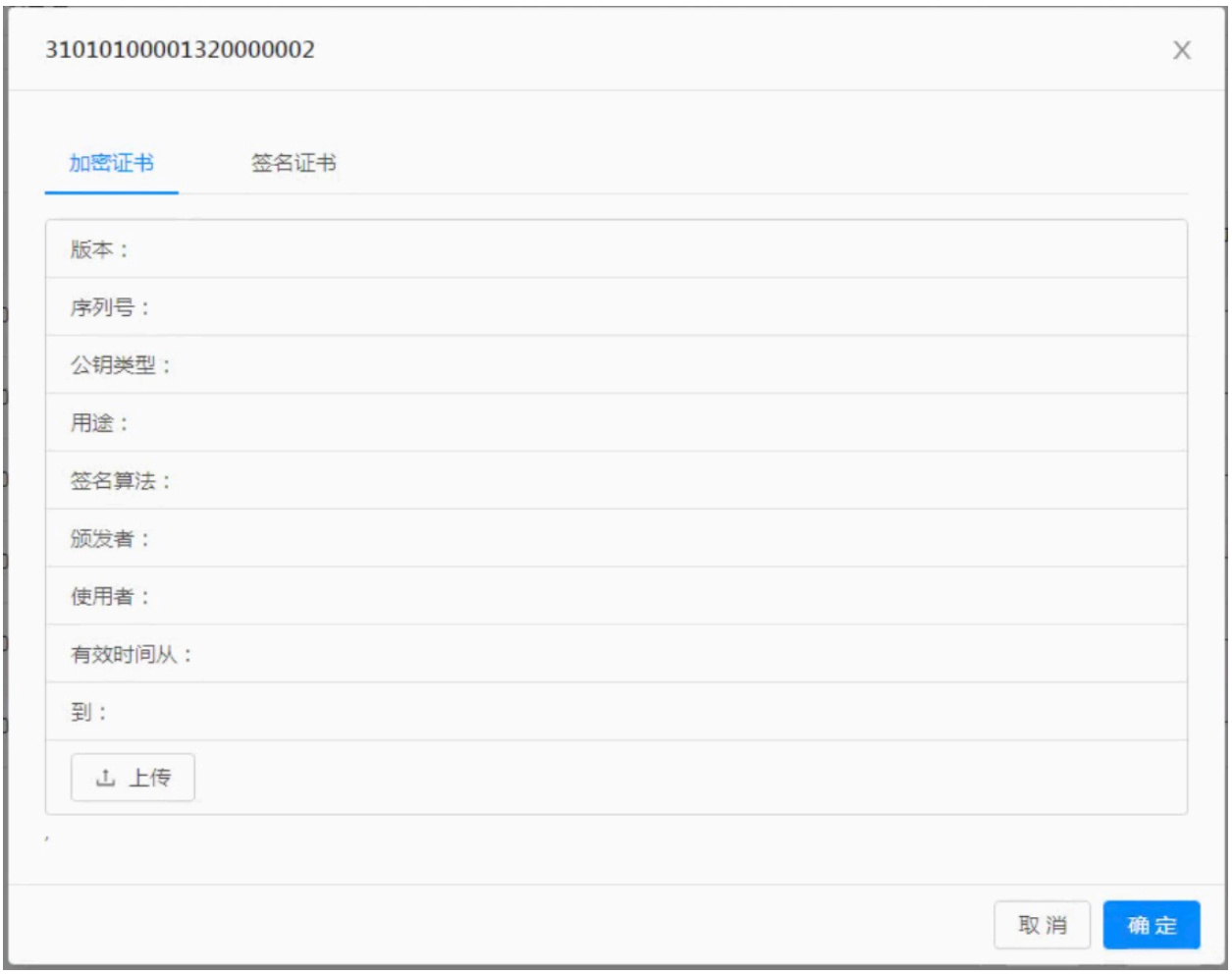
11.3.2 添加相机证书

添加完相机后，需要将相机的证书上传至 SIVS，只有上传完证书后才能正确配置 GB35114 安全功能。（添加 GB/T28181 协议相机，不涉及证书的内容操作，可跳过。）

注：相机证书的获取及给相机发放证书方法，详见“附录二、相机证书发放”。

操作方法：

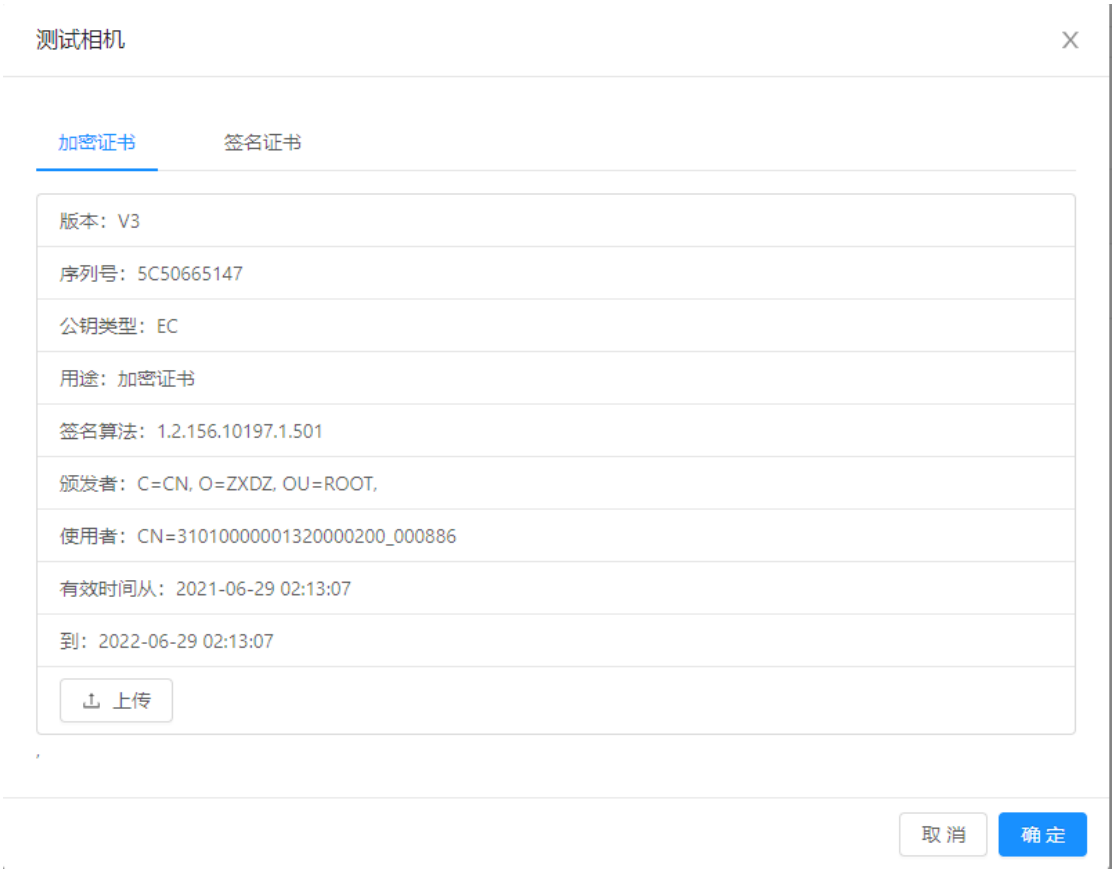
点击对应相机的证书按钮，弹出证书上传对话框。

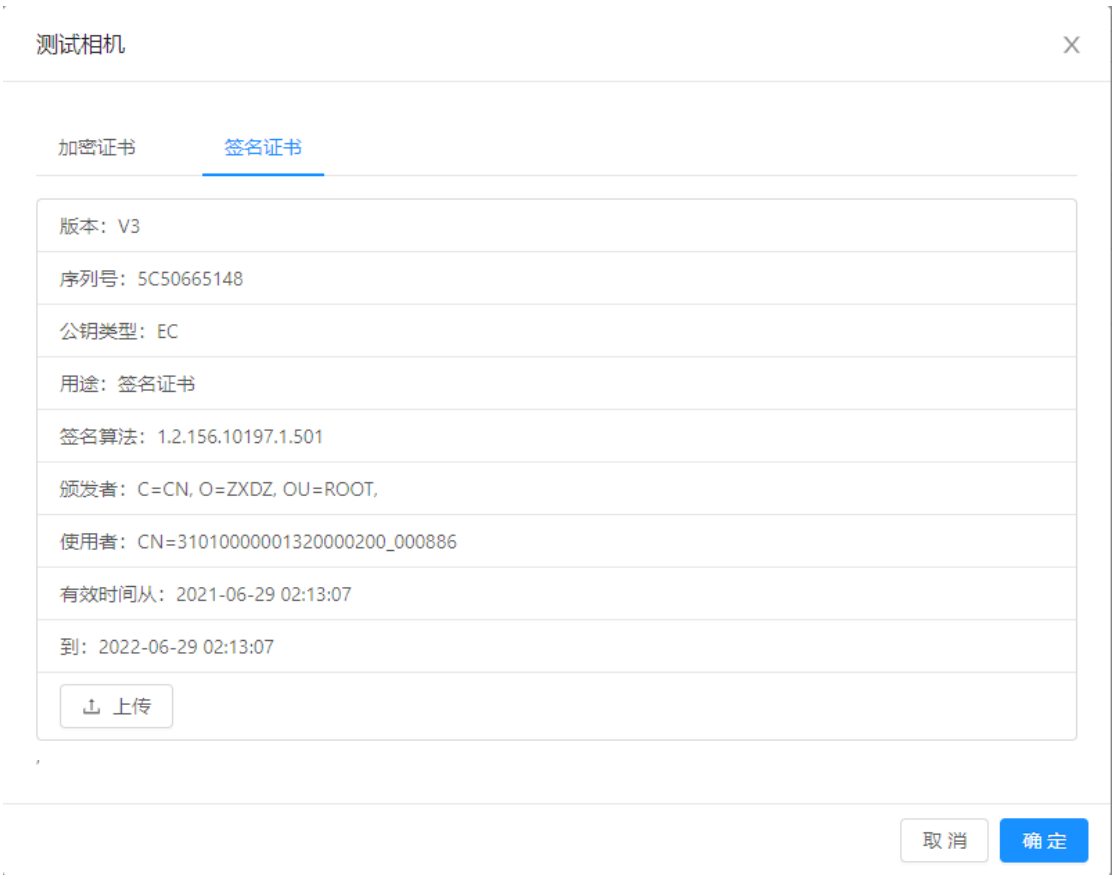


1）、加密证书上传：点击加密证书，点击上传按钮，选择对应相机的加密证书，即可上传相机的加密证书。

2）、签名证书上传：点击签名证书，点击上传按钮，选择对应相机的签名证书，即可上传相机的签名证书。

上传完成后，点击确定按钮。





注：相机证书需要上传 SIVS，同样 SIVS 的证书也要上传相机。操作方法见“附录二、相机证书的发放”。

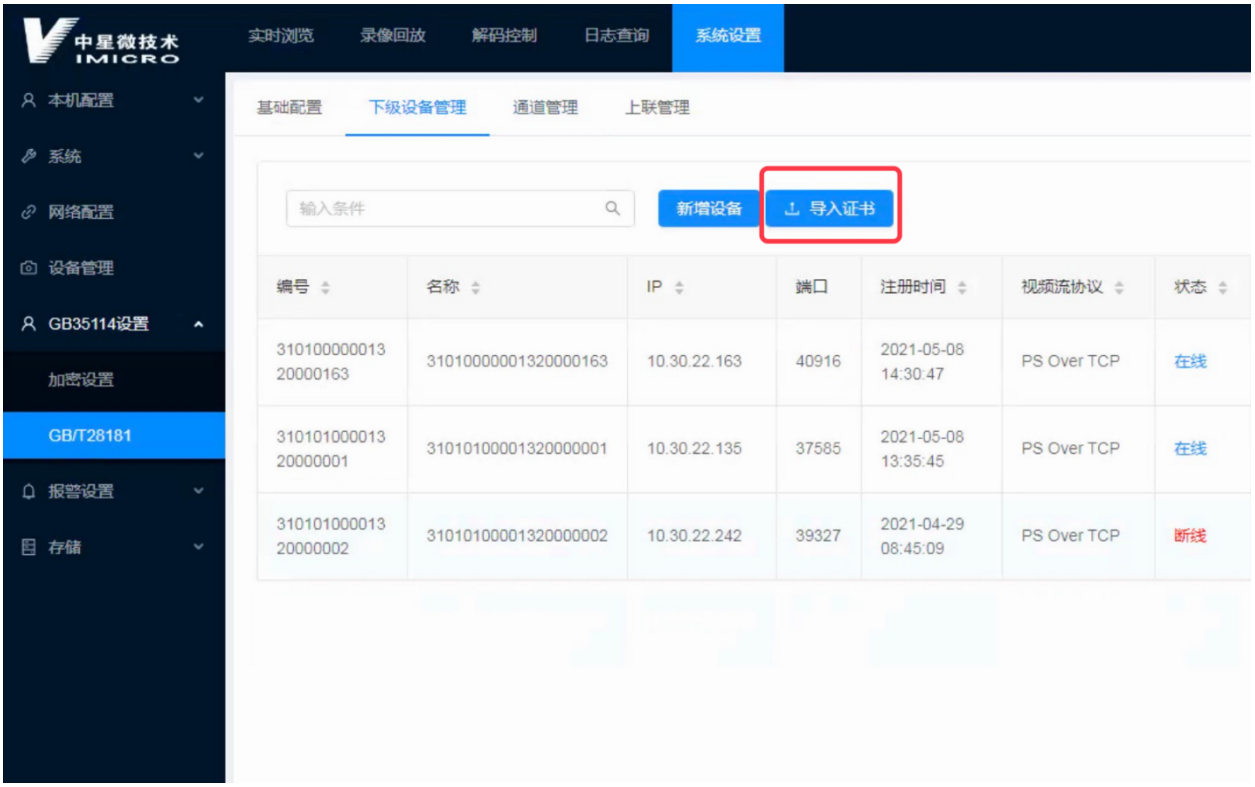
另一种添加证书方法----批量添加相机证书：

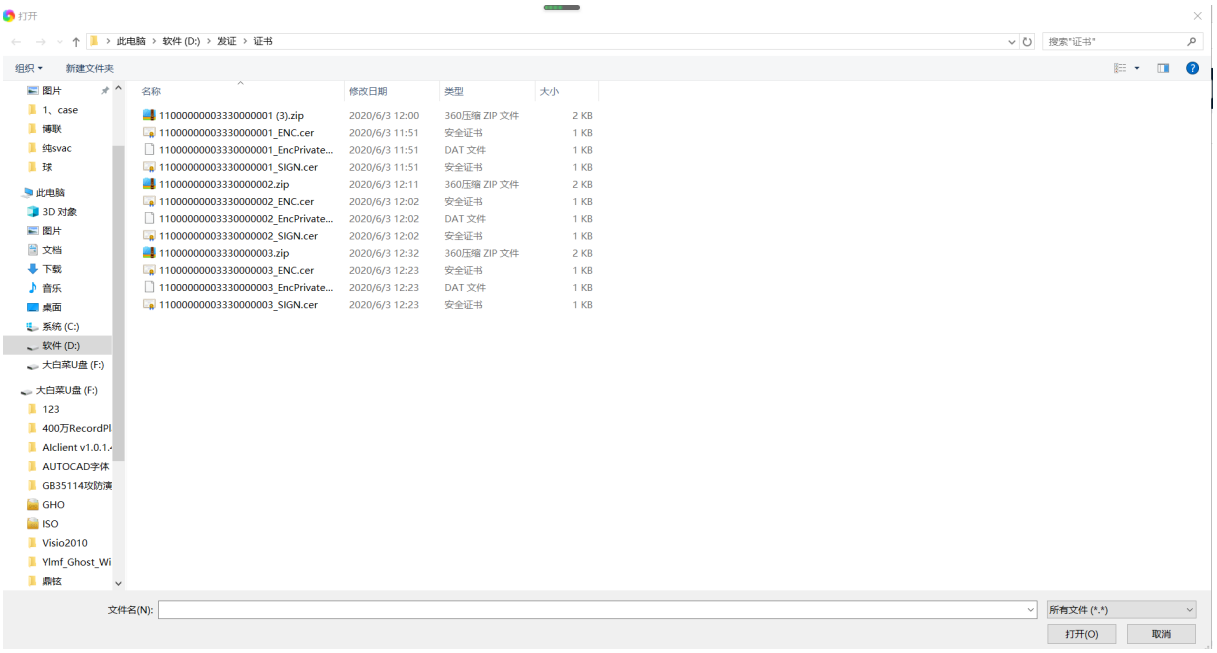
操作方法：

点击对应相机的导入证书按钮，弹出证书上传对话框。选择证书的压缩包，即可批量导入证书。

注：多个证书需提前在 PC 上压缩成一个 zip 文件。右键选中多个证书文件（签名和加密都可），选择“添加到 XXX.zip”。

PC 上安装个压缩软件，即可执行这个操作。



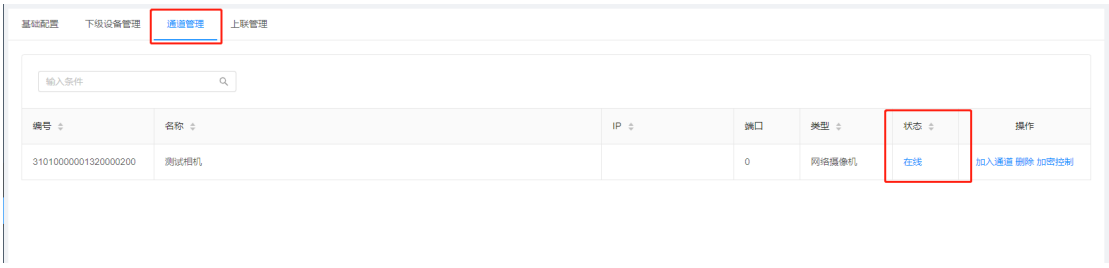


11.3.3 前端相机注册成功

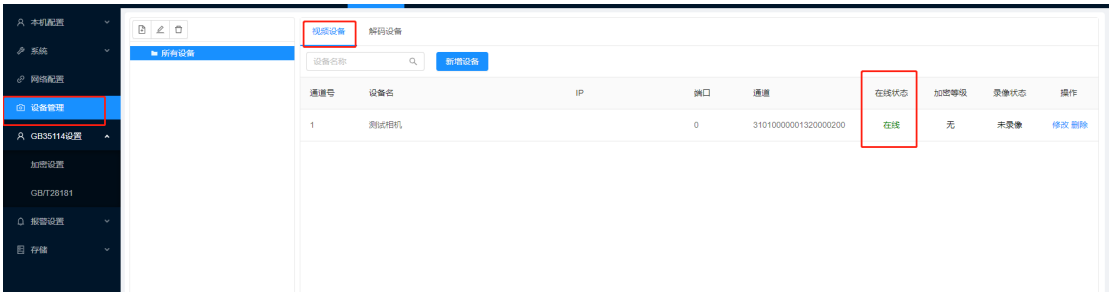
确认前端和 SIVS 相机相应配置完成修改后，刷新页面，等待前端自动重新注册

系统设置→GB35114 设置→GB/T28181→下级设备管理中找到对应前端，状态为“在线”

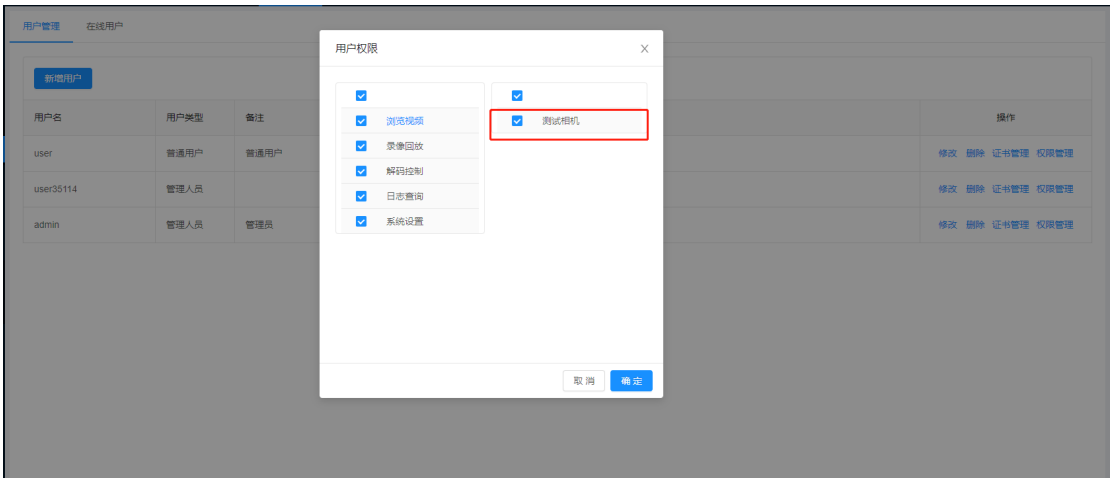
在系统设置→GB35114 设置→GB/T28181→通道管理中找到对应前端，状态为“在线”



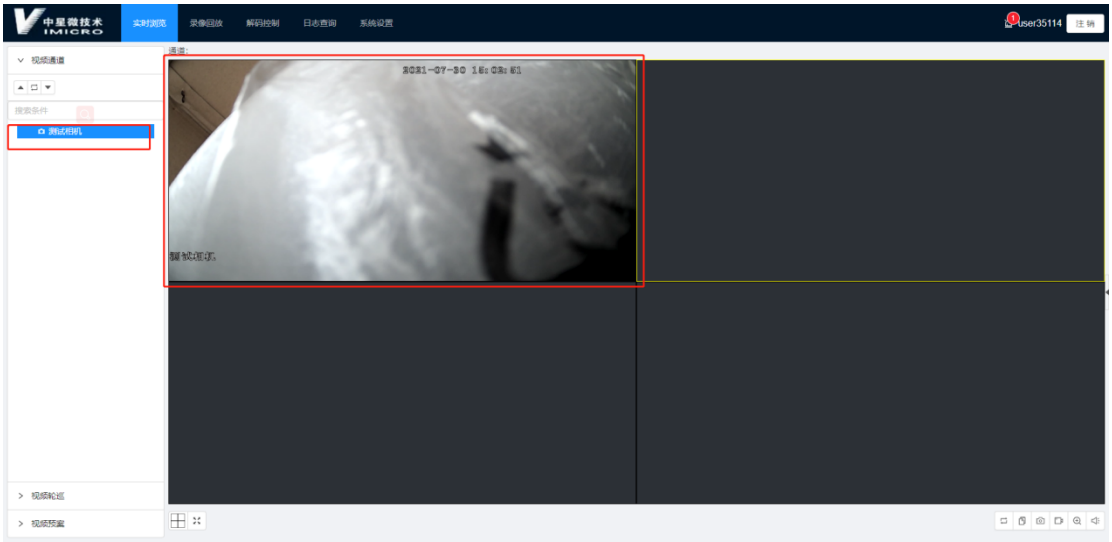
在设备管理→视频设备中找到对应前端，状态为“在线”



此时，我们可以确认前端注册成功，根据前章节描述，添加用户权限，在实时浏览中勾选新添加相机，点击确认



此时，我们可以在实时浏览视频通道中显示该前端相机，并播放该前端视频

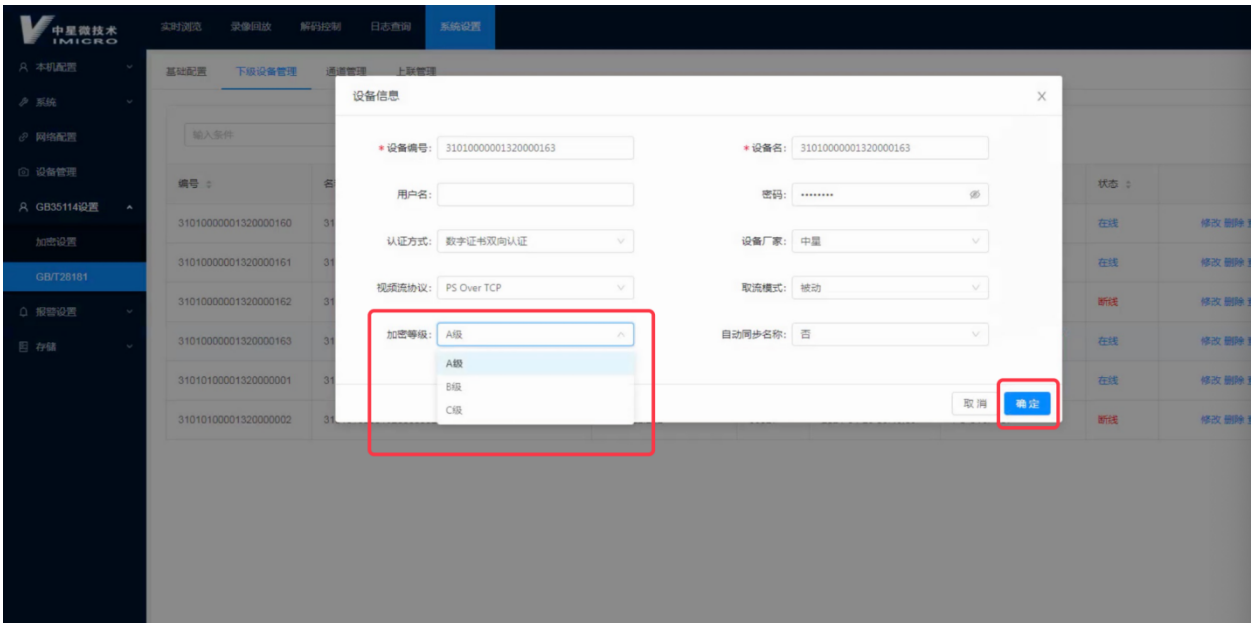


11.3.4 前端相机更改安全等级

SIVS 添加完成相机的证书后，默认只有 A 级，B 级和 C 级需要更改前端相机设置。

操作方法：

点击系统设置→GB35114 设置→GB/T28181→下级设备管理，点击对应前端相机修改按钮。选择加密等级，等待前端重新注册后生效：



11.3.5 前端相机名称修改

操作方法：

点击系统设置→设备管理，进入添加相机界面。

选择需要修改通道名称的相机，点击其后的“修改”，弹出修改对话框。直接在“设备名”后输入新的通道名称，点击确定按钮即可。其他内容不修改。

注：如需手动修改通道名称时，请先在“下级通道管理”中，点击相应相机后的“修改”按钮，将“自动同步名称”选择为“否”，点击“确定”保存后再手动进行通道名称的修改。

11.4 存储

相机添加完成后，需要配置存储，相机才能有录像。本配置项，可以设置 SIVS 录像的存储策略、对存储空间进行格式化和修复操作。

11.4.1 存储管理

11.4.1.1 SIVS708

配置相机的存储策略前首先对新添加的硬盘进行格式化操作。

操作方法：

点击存储→存储管理，选择对应的硬盘，点击格式化按钮，进行格式化。

11.4.1.2 SIVS724

配置相机的存储策略前首先对配置好的 RAID 进行格式化操作。

操作方法：

点击系统设置→存储→存储管理，进入 RAID 存储管理界面，选择对应的 RAID，点击格式化按钮，进行格式化。

注：相机开始存储录像后，不允许进行格式化操作。

11.4.2 计划配置

SIVS708 所有硬盘格式化完成后，开始配置相机的存储策略。

SIVS728 RAID 格式化完成后，开始配置相机的存储策略。

操作方法：

点击存储→计划配置，进入相机存储策略配置界面，选择某一日期后的设置按钮。

弹出“计划设置”对话框。

1）、设置录像的起始和截止时间；

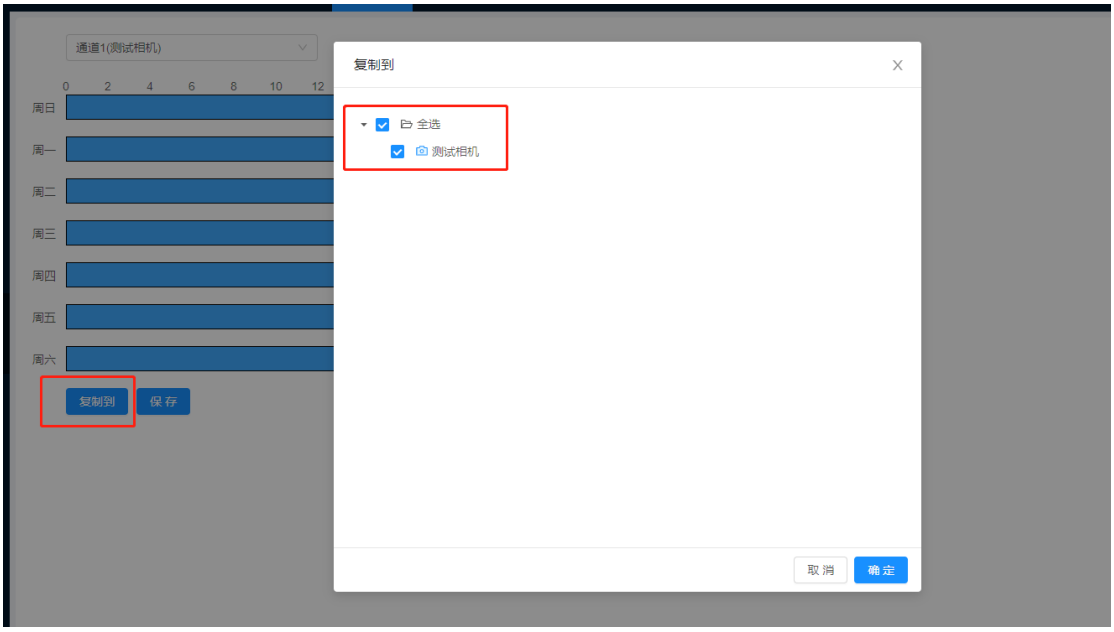
2）、设置录像类型。可选择“正常录像”；

3）、选择起始截止时间、录像使用的日期。可将周日到周六都勾选。

点击确定按钮即可保存。

设置完日期和录像类型后，返回计划配置界面，点击复制到按钮，弹出复制到对话框。在对话框上选择哪些相机按上述的日期和类型进行录像。可以选择所有相机。

注：SIVS 默认只配置第 1 通道，所以其他相机要使用“复制到”功能或单独配置。



点击确定按钮，返回计划配置界面，点击保存按钮，即完成相机的录像存储配置。

12 实时浏览

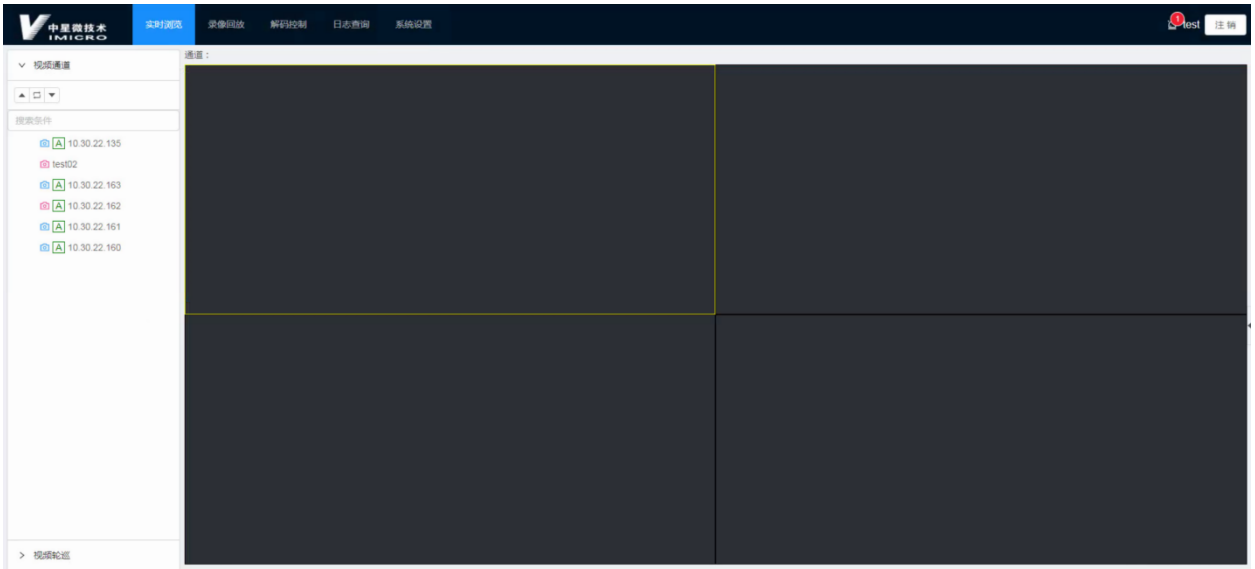
12.1 实时视频

12.1.1 实时视频浏览

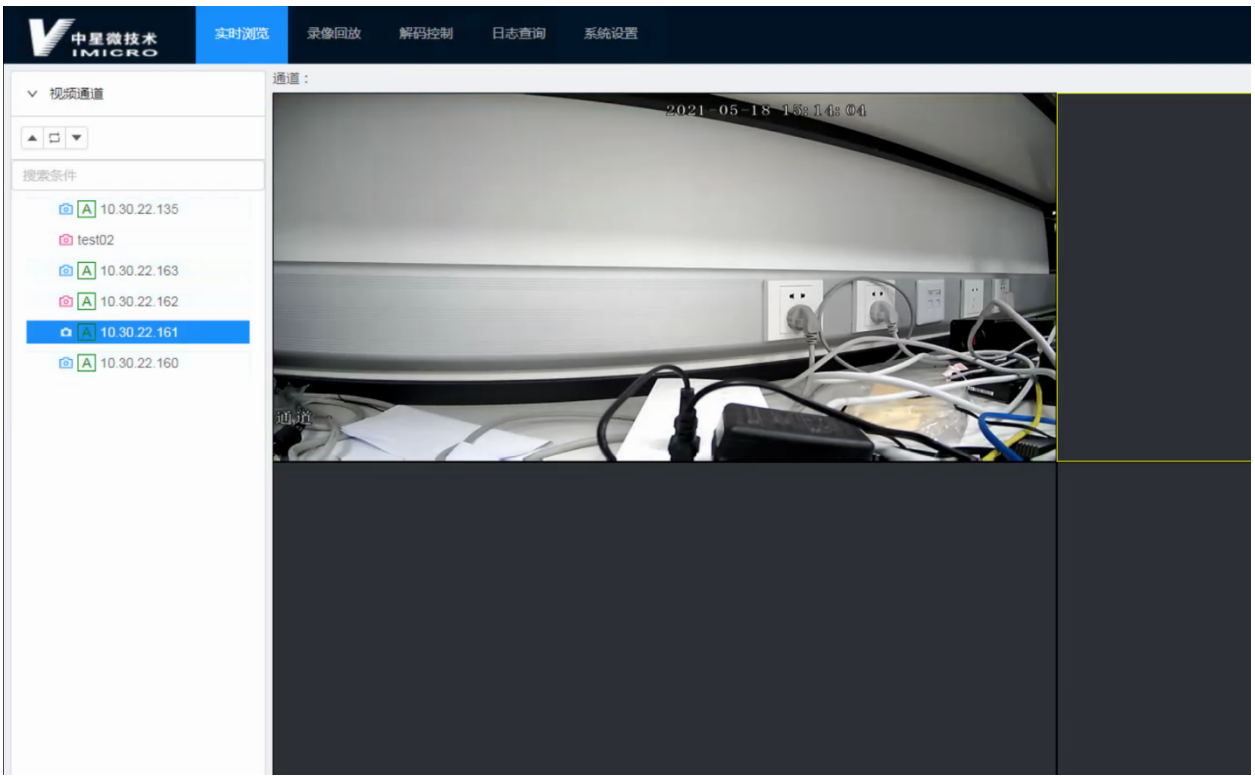
使用 360 极速浏览器（极速模式）登录 SIVS。

注：浏览 GB35114 安全功能 C 级的相机的视频（回放录像）需要使用 USBkey 登录。普通用户名密码登录，只能浏览 GB35114 安全功能的 A 级、B 级、及普通 GB/T28181 相机视频（回放录像）。

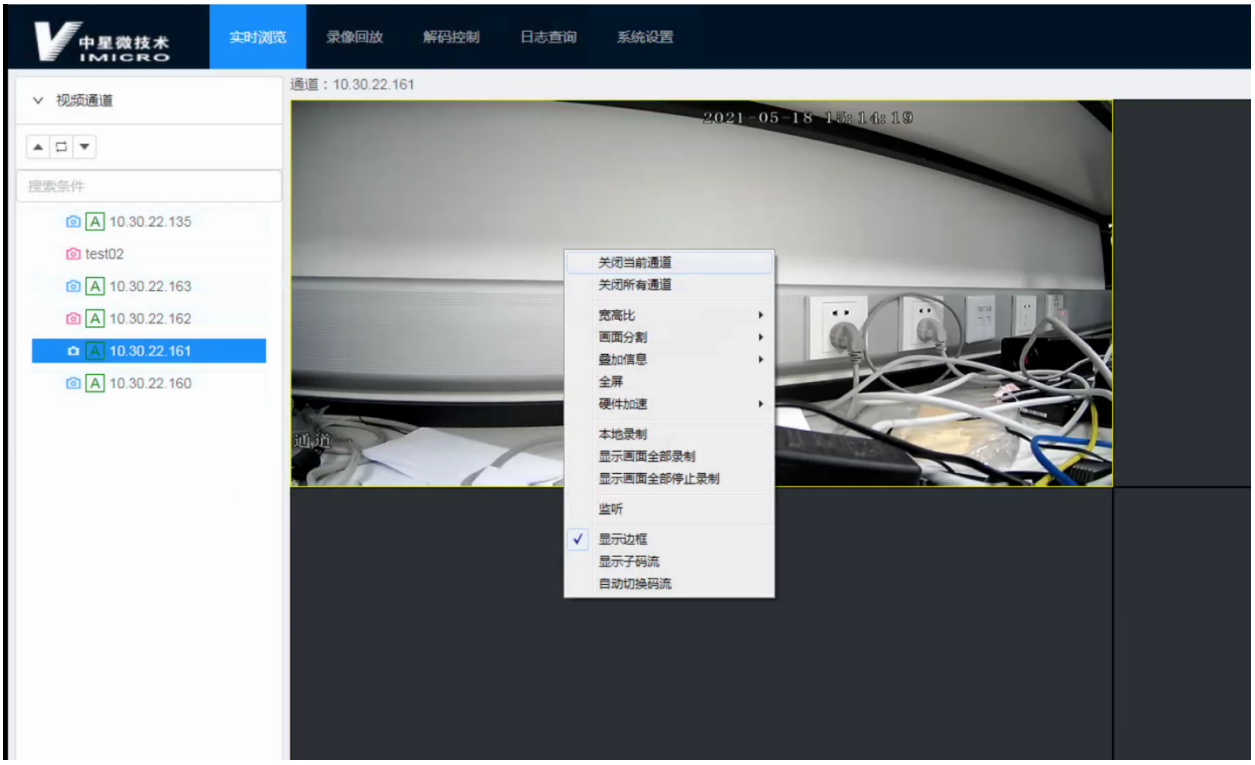
使用 USBkey 登录 SIVS。（SIVS 登录，请参考“ SIVS 登录”章节。）如下图。



在中间显示区域选择需要显示的窗口，在左侧设备列表选择需要浏览的相机，双击此相机：



关闭视频，在显示画面上右键，选择“关闭当前通道”或“关闭所有通道”：



无论是 GB35114 安全功能的 A 级、B 级、C 级视频还是普通 GB/T28181 接入的视频，在 SIVS 上浏览视频的操作都是一样的。

12.1.2 前端相机的安全等级显示

1、普通 GB/T28181 相机和 GB35114 安全功能方式接入的相机的区别：

1）、普通 GB/T28181 相机。在“添加相机”章节，添加相机时认证方式为“密码认证”,且相机在“附录一、相机配置”中不启用“双向认证”（双向认证设置为“强制关闭”。），为普通 GB/T28181 相机。

2）、GB35114 安全功能方式接入的相机。在“添加相机”章节，添加相机时认证方式为“数字证书双向认证”，且相机按“附录一、相机配置”中启用“双向认证”，为 GB35114 安全功能方式接入的相机。

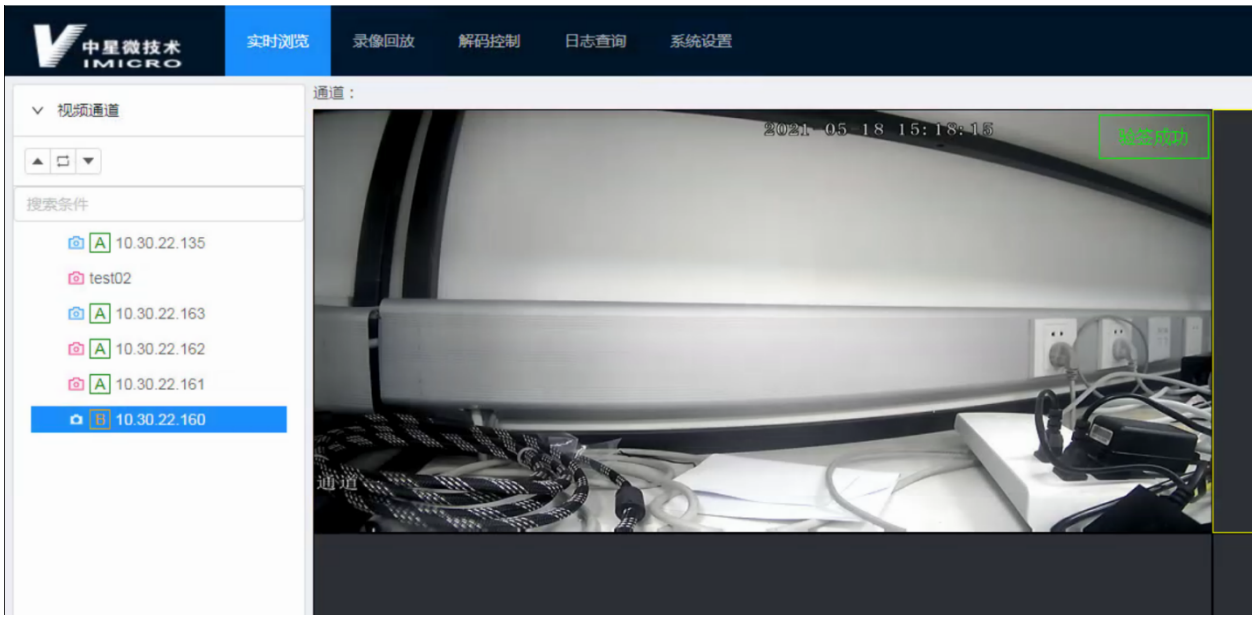
2、GB35114 安全功能的 A 级、B 级、C 级区别方法：

1）、A 级。在“添加相机”章节，添加相机时认证方式为“数字证书双向认证”，且相机按“附录一、相机配置”章节内容进行配置，SIVS 默认为 A 级。

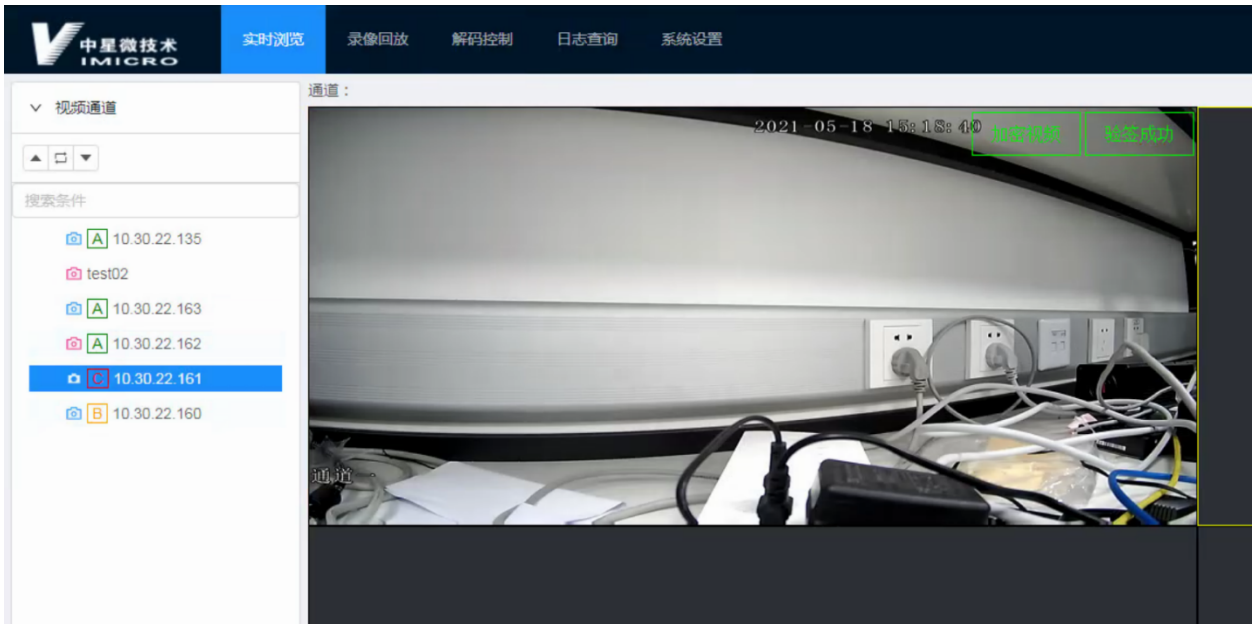
2）、在“前端相机更改安全等级”章节，启用视频签名则为 B 级，启用视频加密则为 C 级。

A 级视频在 SIVS 客户端上打开后的表现形式 和普通 GB/T28181 视频显示形式一样，如下图。

B 级视频在 SIVS 客户端上打开后的表现形式，会显示“验签成功”，如下图。



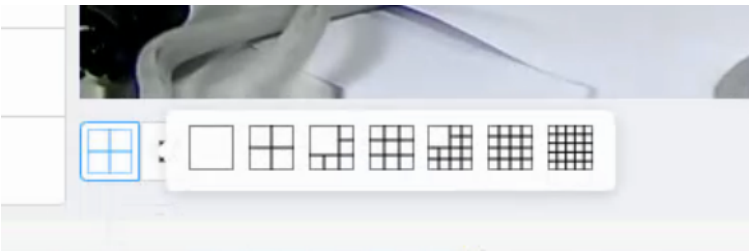
C 级视频在 SIVS 客户端上打开后的表现形式，会显示“加密视频”和“验签成功”，如下图。



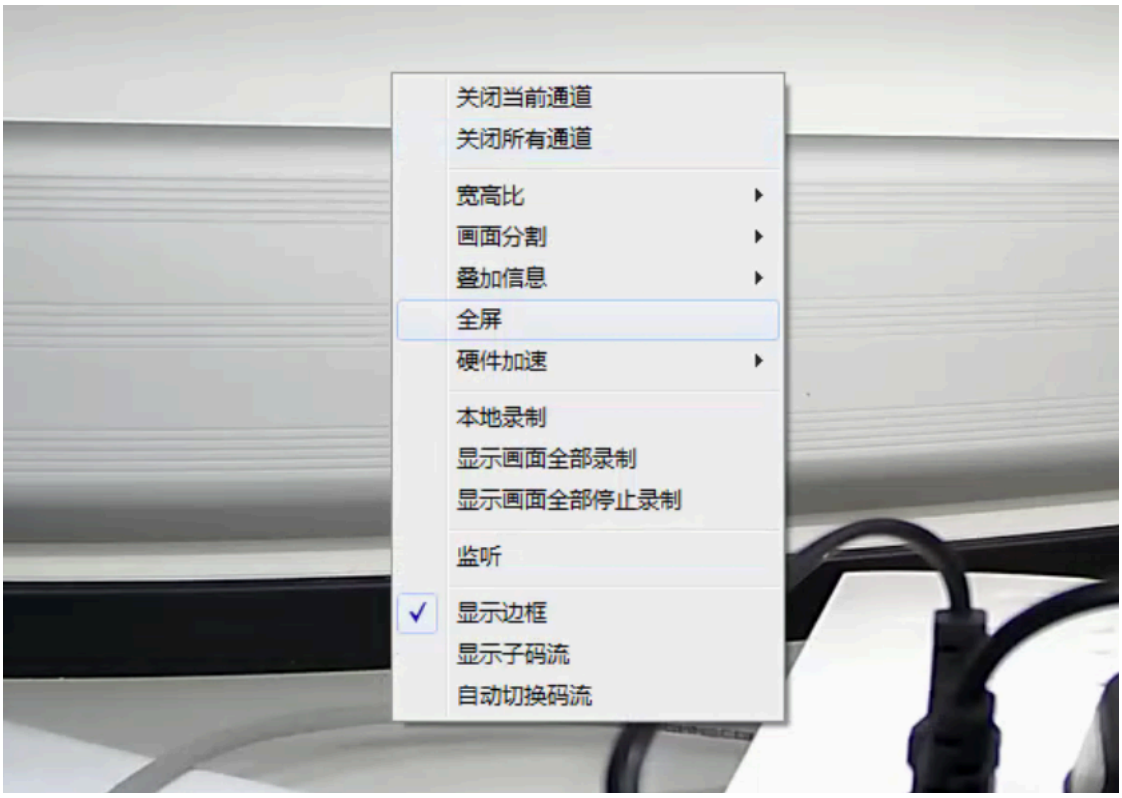
12.1.3 视频浏览基本功能

实时视频可支持关闭通道功能，宽高比、画面分割、叠加信息、全屏功能、硬件加速功能、本地录制、显示画面全部录制、监听、显示边框、显示子码流、自动切换码流等，如下图。

A、点击按钮可以进行分屏选择，分屏数量主要分为 1、4、6、9、13、16、25 具体需求根据自己需要来定，单击选择分屏数量：



B、点击按钮，实现全屏功能，双击视频放大，也可缩小，全屏时若想退出，右击视频，点击全屏选项方可退出全屏：

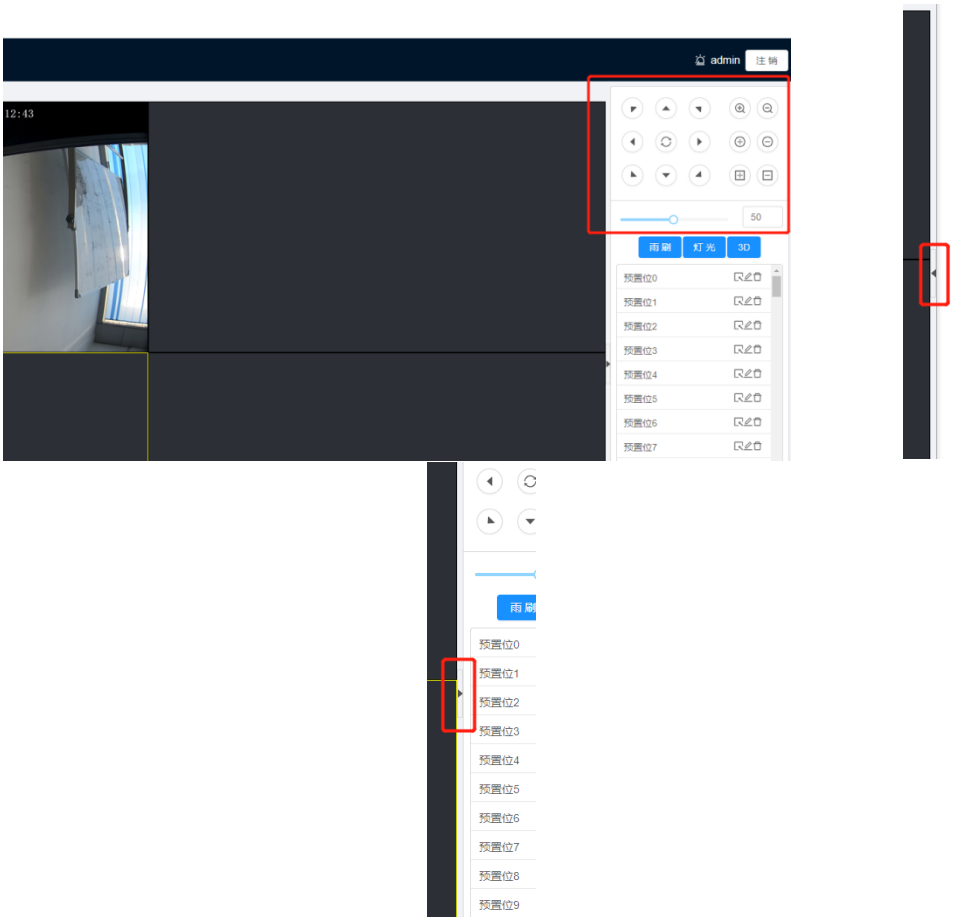


C、画面上右键，选择本地录像，进行本地录像操作，当视频画面出现红色和白色 rec 字样时，即表示视频正在进行录像功能的操作，再次点击可停止录像操作。

默认保存在系统设置→本机配置→本机参数，中设置的路径，见下图：

12.1.4 云台功能

云台功能：选中需要调节方向的视频通道，点击云台控制器上的方向按钮，方向按钮包括：上、下、左、右、左上、右上、左下、右下、放大，缩小、聚焦、散焦、光圈大、光圈小等功能（云台功能仅支持可以调试且带有这些功能的前端绑定设备）：



注：SIVS 默认界面云台操作界面是右侧隐藏，需要手动点开

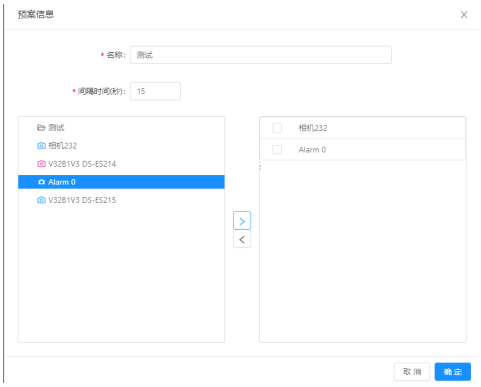
12.2 视频轮巡

12.2.1 添加视频轮巡

1、点击视频轮巡选项，选择并点击“ ”键（新建轮巡）。

2、出现添加视频轮巡对话框，填写轮巡名称、设置轮巡时间间隔、将需要轮巡的相机从左侧添加到右侧，点击确定按钮保存。如下图：

3、轮巡设置完成后。点击应用轮巡按钮，即可启动轮巡功能，如下图：



12.2.2 修改视频轮巡

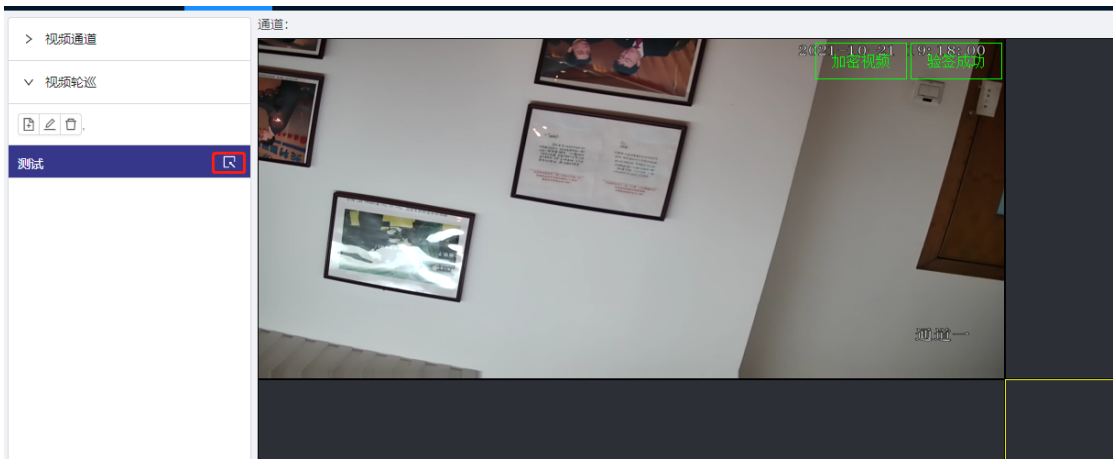
点击修改轮巡按钮，见下图。修改轮巡界面和添加轮巡界面，请参考“3.2.1 添加视频轮巡”章节。

12.2.3 删除视频轮巡

选中已添加的视频轮巡，点击“ ”键进行删除，点击确定即可删除。如下图所示：

12.2.4 应用轮巡

选中需要应用的轮巡，点击“ ”键进行轮巡。如下图所示：

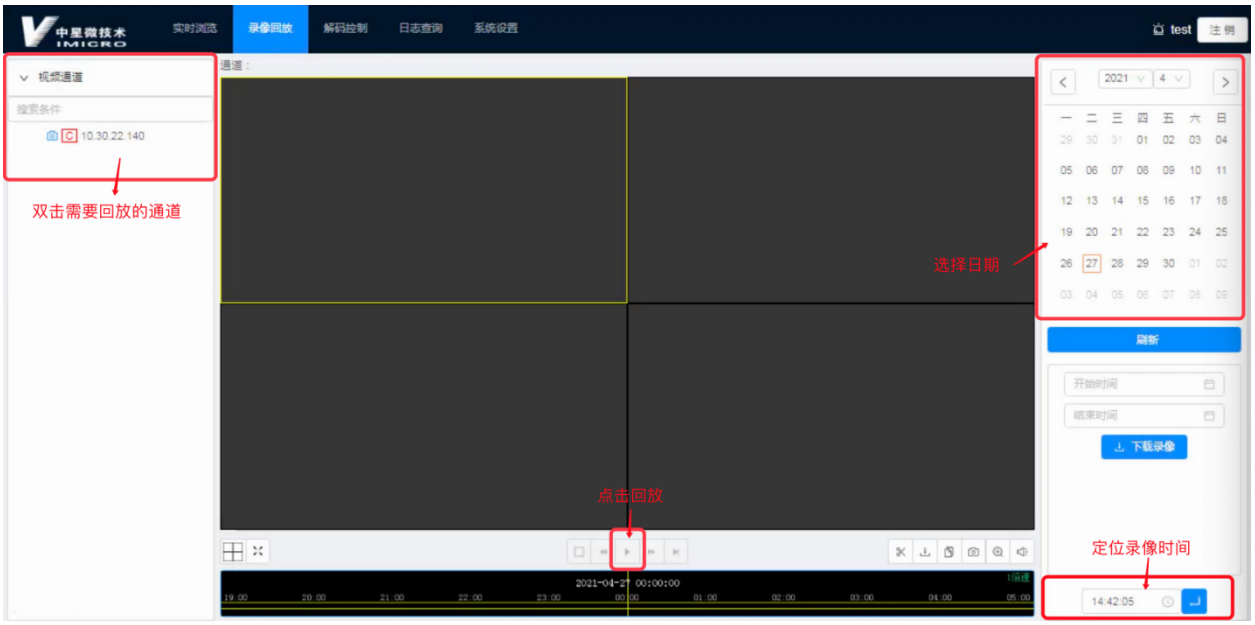


13 录像回放

13.1 录像回放功能

支持视频放大，全屏，抓拍，电子放大，监听，以及倍速播放等功能，其基本操作基本与实时浏览功能相同。

选择回放的日期，双击需要回放的相机通道，设置录像定位时间，然后点击回放。如下图。



13.2 前端相机的录像安全等级显示

GB35114 安全功能 A 级相机的录像也是 A 级；同理 B 级相机的录像也是 B 级、C 级相机的录像也是 C 级；普通 GB/T28181 相机的录像为普通录像，不具备 GB35114 安全功能。

区别方法：请参考“前端相机的安全等级显示”章节。

13.3 录像下载功能

选择开始时间和结束时间，点击“下载录像”，即可进行录像下载，默认保存在 C:\bl\download 文件夹下。

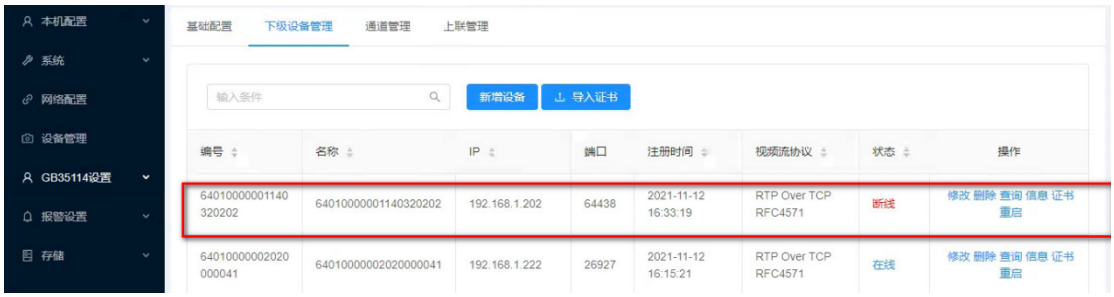
14 解码设备配置与投屏

14.1 系统自动添加解码设备

操作方法：

按照附录五的指导，完成解码设备配置，此时解码设备会主动向 SIVS 进行注册。

点击系统设置→GB35114 设置→GB/T28181→下级设备管理，找到自动注册的解码设备信息



点击修改（同相机修改）

选择和填写以下相应内容：

1）、设备编号。填写解码设备的国标 ID。

2）、设备名。即解码设备的名称。

3）、用户名。需与解码设备国标对接配置中的设备号一致。

3）、密码。需与解码设备国标对接配置一致。默认：12345678。详见“附录五、解码设备配置及证书导入”。

4）、认证方式。添加 GB/T28181 协议解码设备选择“密码认证”；添加 GB35114 安全功能解码设备，选择“数字证书双向认证”。

5）、设备厂家。选择“中星”或按实际接入情况选择。

6）、视频流协议。选择“UDP”。

7）、取流模式。选择“被动”。

8）、自动同步名称。选择“否”。

点击确定进行保存。

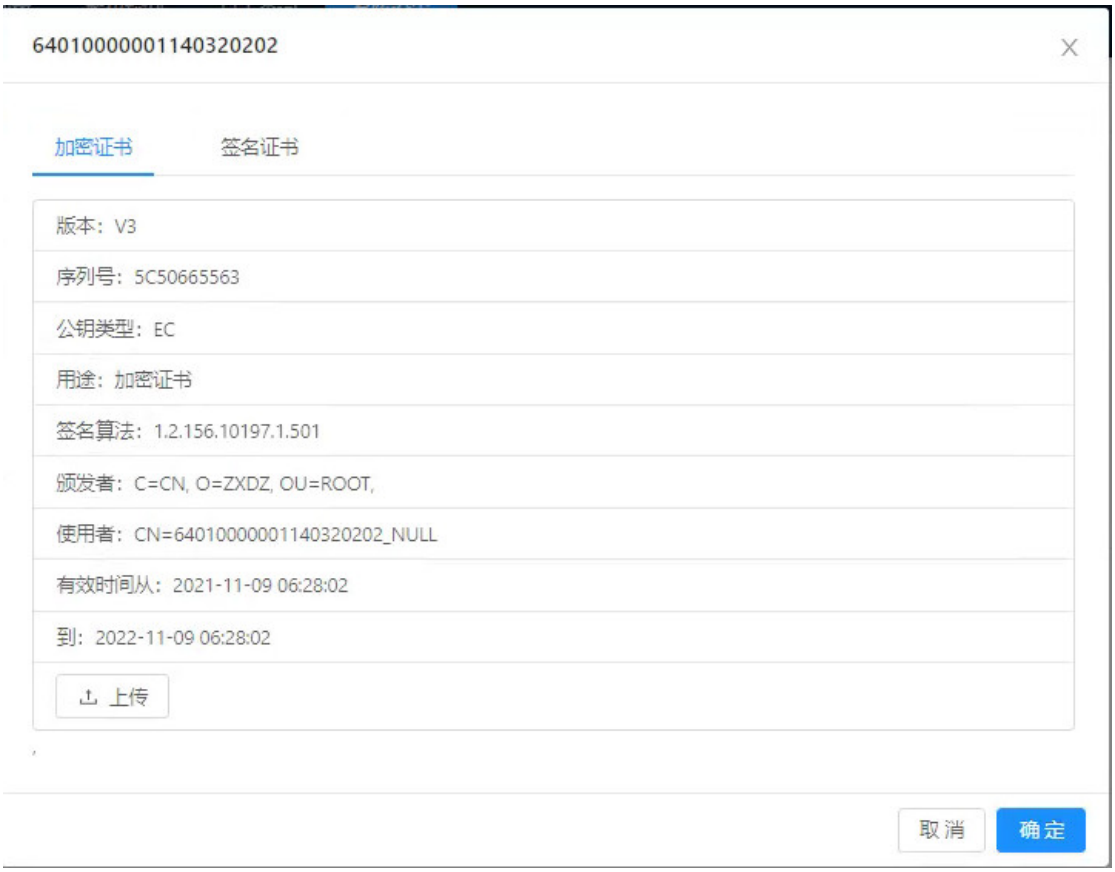
14.2 添加解码设备证书

添加完解码设备后，需要将解码设备的证书上传至 SIVS，只有上传完证书后才能正确配置 GB35114 安全功能。（添加 GB/T28181 协议相机，不涉及证书的内容操作，可跳过。）

注：解码设备证书的获取及给解码设备发放证书方法，详见“附录五、解码设备配置及证书配置”。

操作方法：

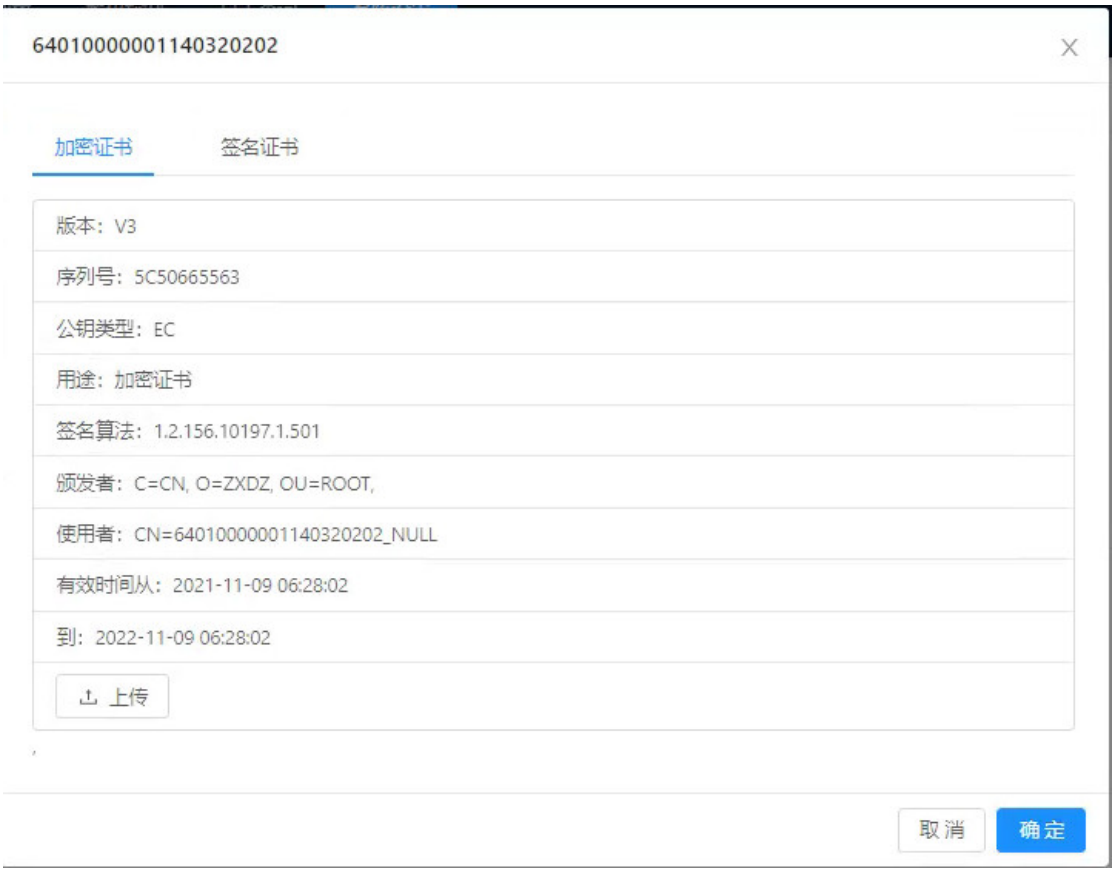
点击对应解码设备的证书按钮，弹出证书上传对话框。

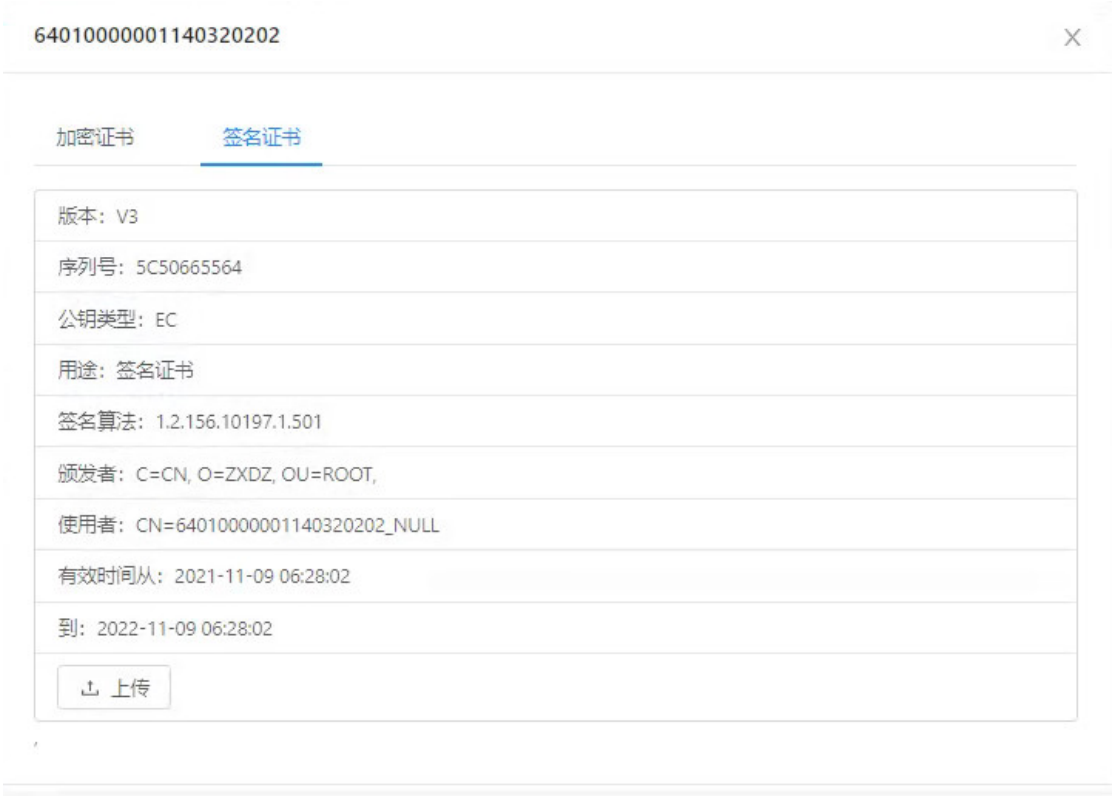


1）、加密证书上传：点击加密证书，点击上传按钮，选择对应解码设备的加密证书，即可上传解码设备的加密证书。

2）、签名证书上传：点击签名证书，点击上传按钮，选择对应解码设备的签名证书，即可上传解码设备的签名证书。

上传完成后，点击确定按钮。


64010000001140320202
加密证书
签名证书
版本：V3
序列号：5C50665563
公钥类型：EC
用途：加密证书
签名算法：1.2.156.10197.1.501
颁发者：C=CN, O=ZXDZ, OU=ROOT,
使用者：CN=64010000001140320202_NULL
有效时间从：2021-11-09 06:28:02
到：2022-11-09 06:28:02
上传
取消
确定


64010000001140320202
加密证书
签名证书
版本：V3
序列号：5C50665564
公钥类型：EC
用途：签名证书
签名算法：1.2.156.10197.1.501
颁发者：C=CN, O=ZXDZ, OU=ROOT,
使用者：CN=64010000001140320202_NULL
有效时间从：2021-11-09 06:28:02
到：2022-11-09 06:28:02
上传

注：解码设备证书需要上传 SIVS，同样 SIVS 的证书也要上传解码设备。操作方法见“附录五、解码设备配置及证书配置”。

14.3 解码设备注册成功

确认解码设备和 SIVS 解码设备相应配置完成修改后，刷新页面，等待前端自动重新注册

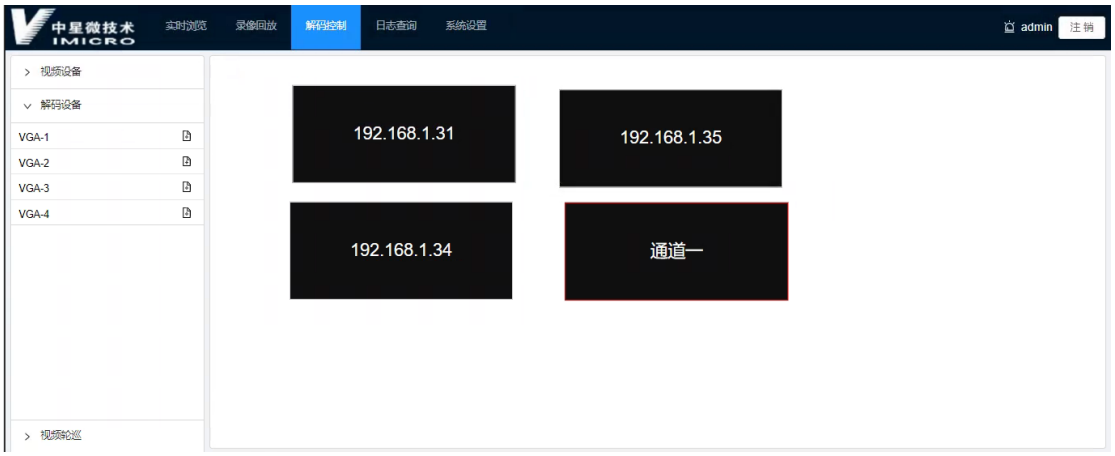
系统设置→GB35114 设置→GB/T28181→下级设备管理中找到对应前端，状态为“在线”

在系统设置→GB35114 设置→GB/T28181→通道管理中找到对应解码设备，状态为“在线”

在设备管理→解码设备中找到对应解码设备，状态为“在线”

此时，我们可以确认解码设备注册成功，根据前章节描述，添加用户权限，在实时浏览中勾选新添加解码设备，点击确认

此时，我们可以在实时浏览视频通道中显示该解码设备，并投屏前端视频

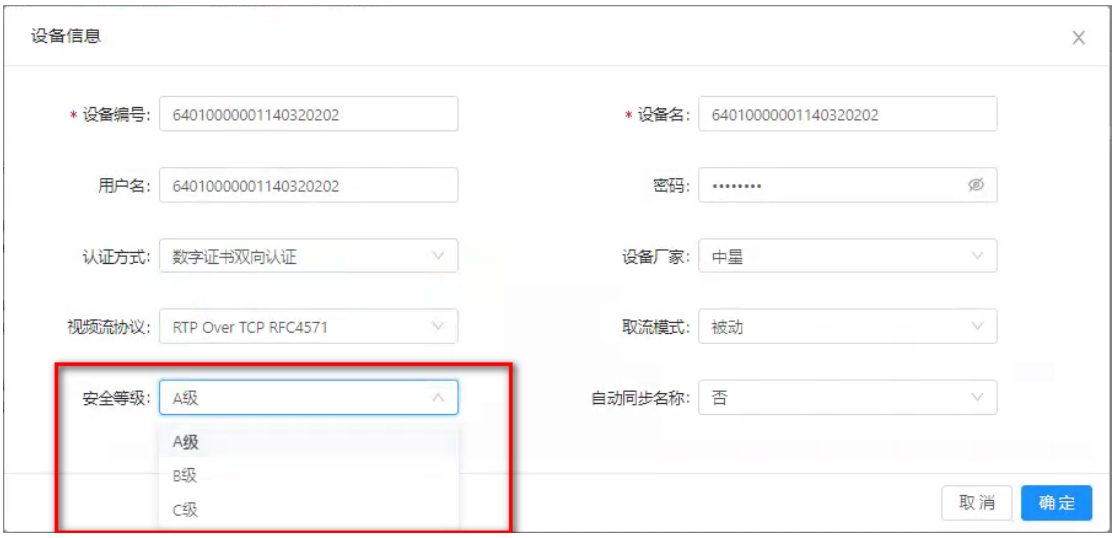


14.4 解码设备更改安全等级

SIVS 添加完成解码设备的证书后 默认只有 A 级 ,B 级和 C 级需要更改解码设备设置。

操作方法：

点击系统设置→GB35114 设置→GB/T28181→下级设备管理，点击对应解码设备修改按钮。选择加密等级，等待前端重新注册后生效：



14.5 解码设备名称修改

操作方法：

点击系统设置→设备管理，进入添加解码设备界面。

选择需要修改名称的解码设备，点击其后的“修改”，弹出修改对话框。直接在“设备名”后输入新的名称，点击确定按钮即可。其他内容不修改。

注：如需手动修改通道名称时，请先在“下级通道管理”中，点击相应解码设备后的“修改”按钮，将“自动同步名称”选择为“否”，点击“确定”保存后再手动进行通道名称的修改。

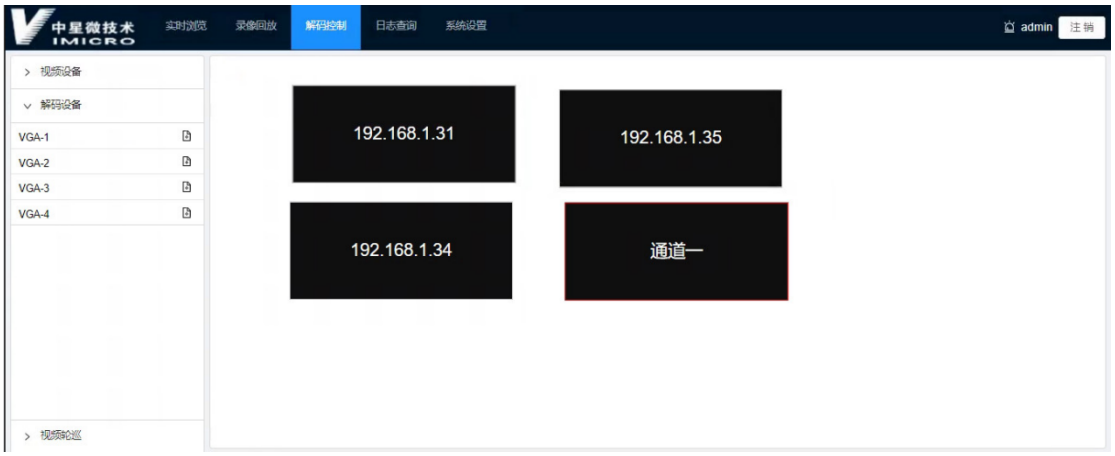
15 解码控制

15.1 添加解码设备

操作方法：

点击解码控制→解码设备，点击 将对应的解码设备添加上。

点击解码控制→视频设备，点击右侧对应的解码器，将左侧的视频设备双击加入解码设备。



16 SIVS 对接 VISS 平台

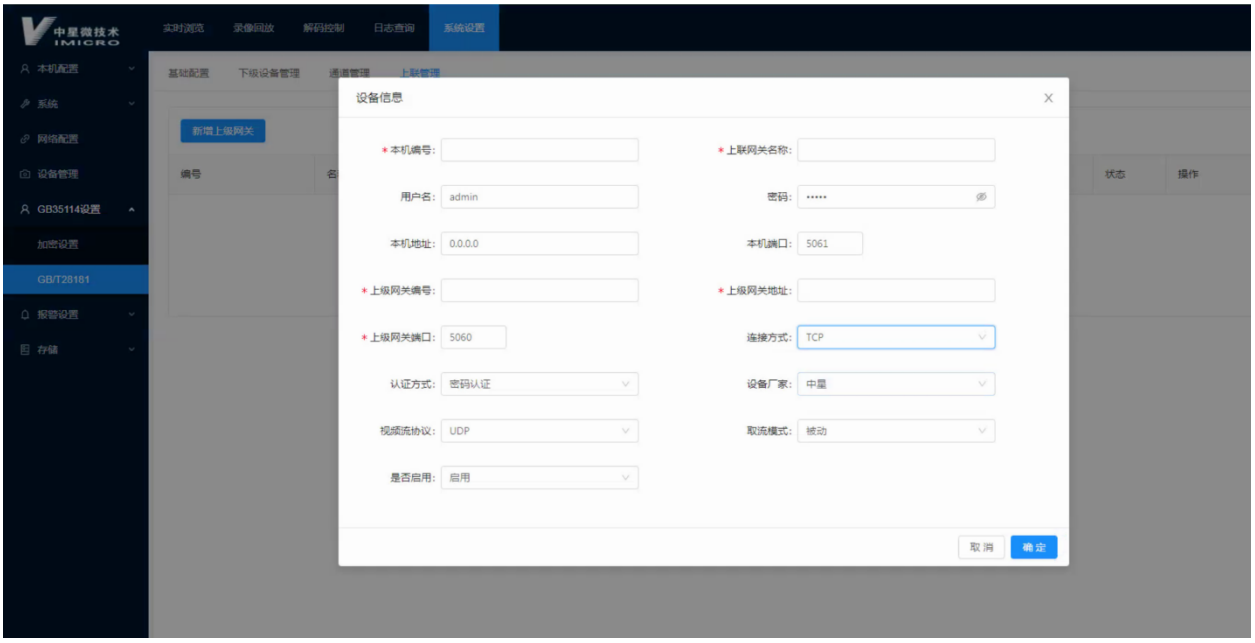
16.1 SIVS 以 GB/T28181 协议接入 VISS

16.1.1 SIVS 配置

操作方法：

点击系统设置→GB35114 设置→GB/T28181→上联管理，进入上联管理界面。

点击新增上级网关弹出对话框，如下图。



配置内容：

本机编号：填写本级 SIVS 的国标 ID；

上联网关名称：填写上级的名称（可以直接填写 SIVS 所对接的 GBFG 的国标 ID）；

用户名：填写本级 SIVS 的国标 ID；

密码：要和 VISS 平台填写的密码一致（通常写：12345678）；

本机地址：SIVS 的 IP 地址；

本机端口：SIVS 的端口（此端口为 SIVS 作为下级时的端口，区别于 SIVS 作为上级时的端口，两者不可一样。）；

上级网关编号：填写 VISS 平台中 SIVS 所对接的 GBFG 的国标 ID；

上级网关地址：填写 VISS 平台中 SIVS 所对接的 GBFG 的 IP 地址；

上级网关端口：填写 VISS 平台中 SIVS 所对接的 GBFG 的国标端口；

连接方式：TCP；（请务必选择 TCP 方式）

认证方式：密码认证；

设备厂家：中星；

视频流协议：UDP；

取流模式：被动；

是否启用：启用。

填写完成后，点击确定。

16.1.2 VISS 配置

1、VISS 操作，请详见 VISS 使用手册；

2、使用 GBFG 对接；

3、VISS 在添加 SIVS 的相机时选择网络相机、录像存储天数可以选择 0。

16.2 SIVS 以 GB35114 安全功能方式接入 VISS

注：VISS 平台需要支持 GB35114 安全功能。即 VISS 平台提前进行 GB35114 安全功能配置。详见 VISS 平台操作手册。

16.2.1 SIVS 配置

SIVS 的 GB35114 安全功能上接 VISS 基于 SIVS 的 GB/T28181 对接 VISS。GB/T28181 对接完成后进行 GB35114 安全功能配置。SIVS 的 GB/T28181 对接 VISS 请参考“5.1.1SIVS 配置”章节内容。

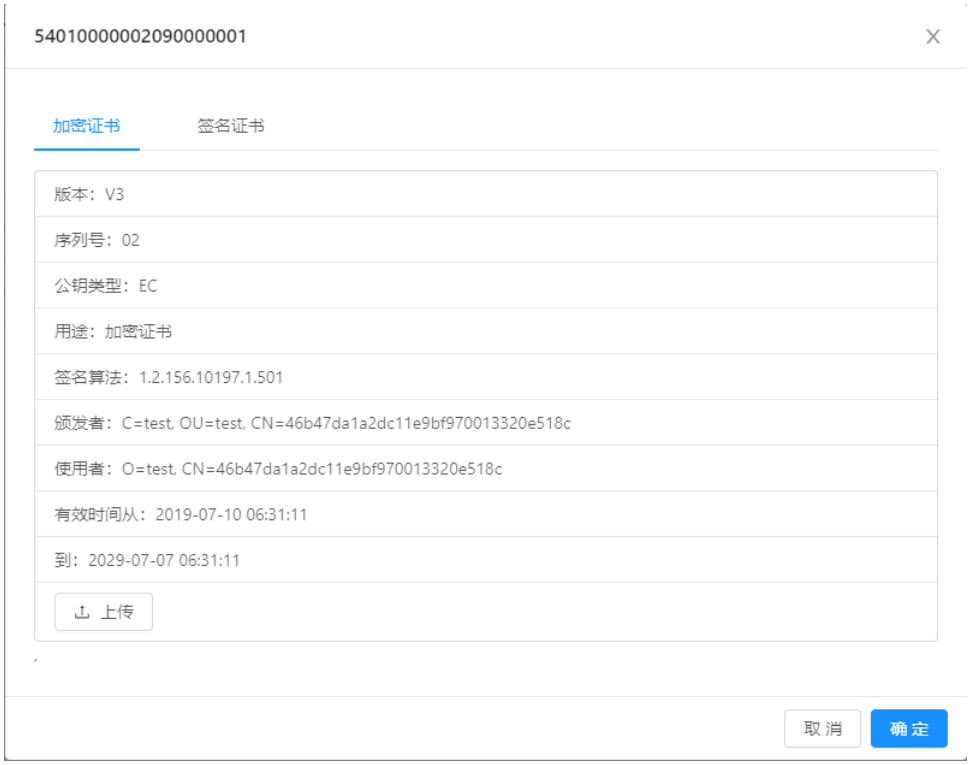
SIVS 的 GB35114 安全功能配置：

操作方法：

点击系统设置→GB35114 设置→GB/T28181→上联管理，进入上联管理界面。

1、选择某一需要设置 GB35114 安全功能的对接项，点击修改，弹出对话框。将认证方式修改为“数字证书双向认证”，点击确定。

2、选择需要设置 GB35114 安全功能的对接项，点击证书管理，弹出对话框。分别上传 SIVS 所对接的 GBFG 的签名和加密证书，点击确定。



注：GBFG 的证书，请与平台技术人员索要。

16.2.2 VISS 配置

1、VISS 操作，请详见 VISS 使用手册；

2、使用 GBFG 对接；

3、VISS 在添加 SIVS 的相机时选择网络相机、录像存储天数可以选择 0；

4、VISS 在添加 SIVS 的相机时，相机的加密和签名证书需要导入 VISS。

附录一、相机配置

注：本文档只讲述相机的 GB/T28181 对接设置和 GB35114 安全功能对接设置。相机其他设置请参考相机操作手册。

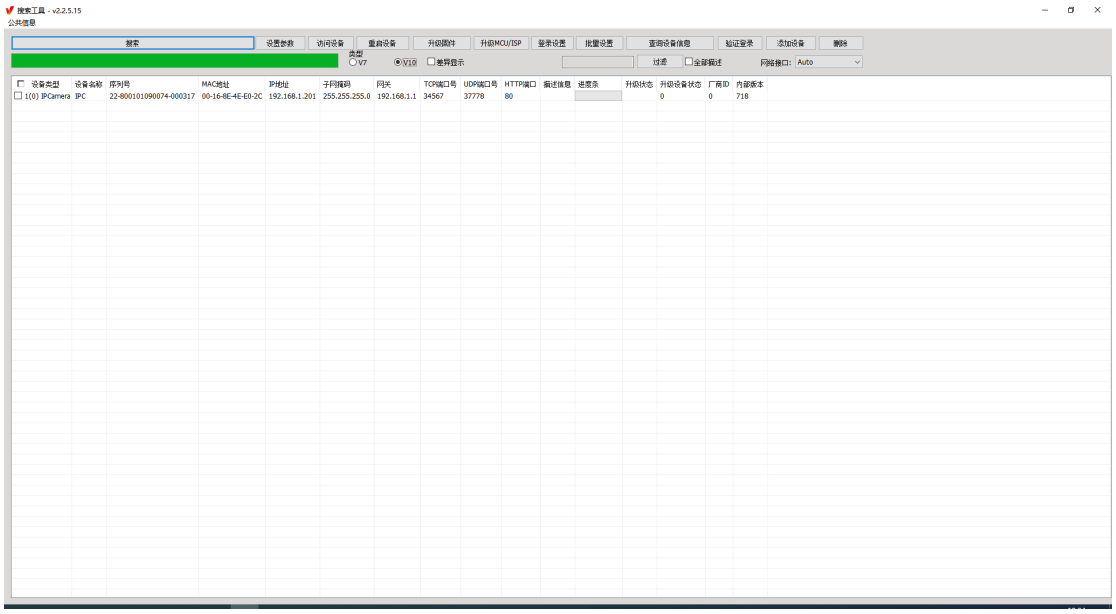
注：本文档只讲述中星微技术的相机对接配置内容，其他厂家相机的配置内容，请与相关厂家技术进行联系。

注：中星微相机，使用前，请和技术人员确认版本是否为最新，版本老旧的相机，请先升级新版本。

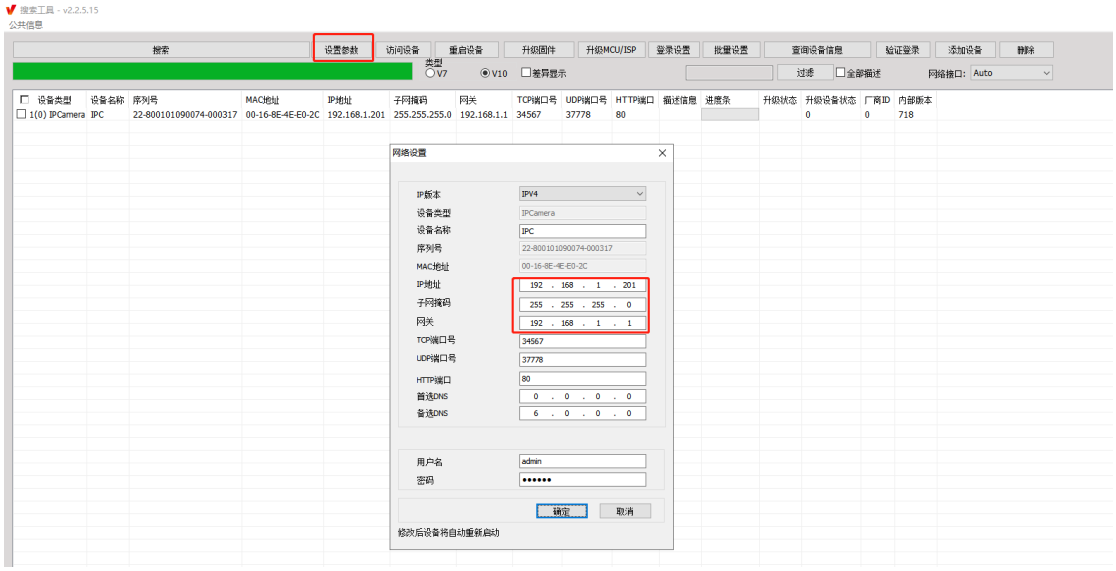
相机实现 GB35114 安全功能，基于 GB/T28181 协议，所以需要提前规划好相机和平台（或 SIVS）的国标 ID 等相关信息。

操作步骤：

1、打开 AutoSearch 搜索工具，点击“搜索 “，搜索出中星微相机，如下图



2、选择下面相应的相机信息，点击“设置参数”修改设备 IP 地址，弹出网络设置对话框；



3、IE 浏览器地址栏中输入中星微相机的 IP 地址，然后敲回车键。若是第一次访问设备，会弹出安装插件的提示对话框，点击【安装】安装插件。安装完毕插件后就会显示登录框。出厂默认用户名：admin,密码：123456

4、登录相机后，首先要将相机的编码格式改为：SVAC2，并保存。如下图。

5、配置相机的 GB/T28181 对接。

相机可以使用“平台接入”或“第二平台”，配置 GB/T28181 内容，用来对接平台（或 SIVS）。“平台接入”或“第二平台”功能相同。

如下图，设置完成后进行保存：

1）、勾选“使能”；

2）、平台协议选择“28181_EX”；

3）、协议传输层选择“TCP”；

4）、“SIP 服务器编号”：填写规划好的服务器国标 ID（或 SIVS 的国标 ID）；

5）、“SIP 服务器 DNS”：填写规划好的服务器的国标域，一般是服务器国标 ID 前十位；

6）、“SIP 服务器 IP”：填写规划好的服务器 IP（或 SIVS 的 IP）；

7）、“SIP 服务器端口”：填写规划好的服务器国标端口（或 SIVS 作为上级的国标端口）；

8）、“设备号”：填写规划好的相机的国标 ID，需与平台（或 SIVS）添加的相机内容一致；

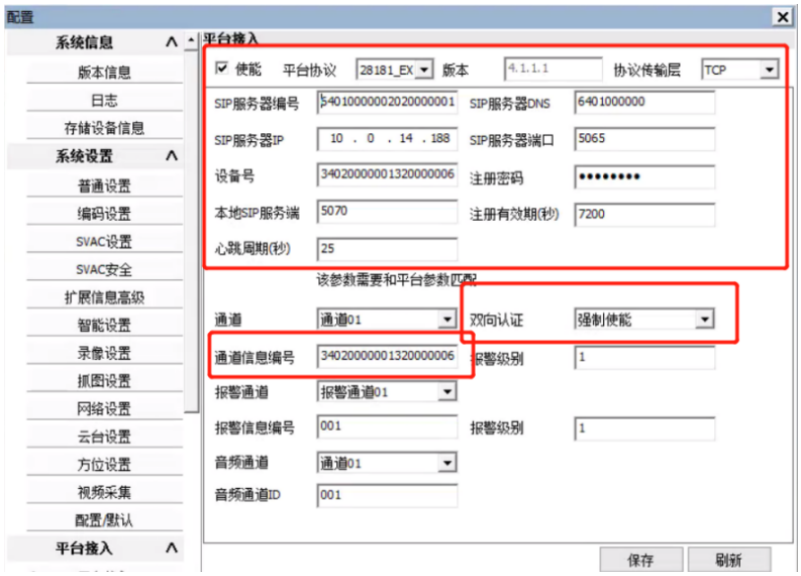
9）、“注册密码”：要与平台（或 SIVS）添加相机时填写的密码一致；

10）、“本地 SIP 服务端”：填写规划好的相机的本地端口，不可与服务器（或 SIVS）端口相同；

11）、“注册有效期”和“心跳周期”：默认；

12）、“通道信息编号”：填写规划好的相机的通道的国标 ID，需与平台（或 SIVS）添加的相机内容一致；

13）、“双向认证”:如果配置 GB/T28181 对接，设置为强制关闭；如果设置为 GB35114 安全功能对接，则设置为强制使能。



注：SIVS 信息的获取途径，请参考“2.2.1 SIVS 国标 ID 等信息的获取及修改”章节。

3、设置“SVAC 安全”。

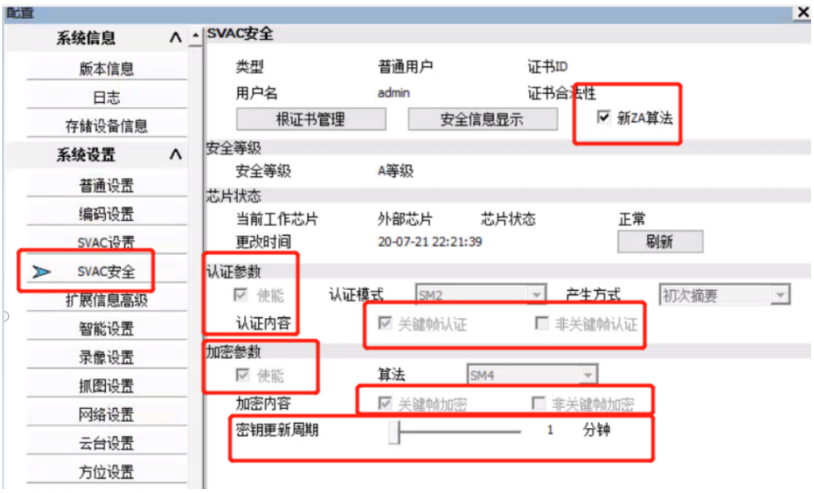
相机的“双向认证”，设置为“强制使能”后，在相机的“系统设置”下会多出“SVAC 安全”设置项。对“SVAC 安全”设置项进行配置。（普通 GB/T28181 对接不需要设置 SVAC 安全。）

1）、勾选“新 ZA 算法”；

2）、“认证参数”，勾选使能。并勾选“关键帧认证”；

3）、“加密参数”：勾选使能。并勾选“关键帧加密”；

4）、“密钥更新周期”：设置为 1 分钟。



点击“保存”后，相机设置完成。

注：需要将平台对接的使能勾选去掉后，才能设置“SVAC 安全”，设置完“SVAC 安全”后，再将平台对接的使能勾选上即可。

附录二、相机证书的导入

所有设备的证书都由 CA 系统来发放，如现场有 CA 系统，可以使用现场的 CA 系统进行证书发放；如现场没有 CA 系统，可联系中星微销售人员进行证书发放。

提取 P10 和导入证书操作方法：

1、提取 P10 文件。

使用浏览器登录相机（相机相关操作，请参考相机的操作手册。），点击系统设置→系统设置→SVAC 安全→证书管理，进入证书管理界面。

在 P10 提取部分设置和操作以下内容项，如下图：

国标 ID，填写相机的国标 ID；

输出路径，设置 P10 文件存在 PC 上的位置；

输出格式，设置 P10 文件的格式，卫士通选择 DER、信安选择 PEM，目前仅支持这两种。

设置完成后，点击 P10 导出，即可正常导出相机的 P10 文件。

注：P10 文件选择卫士通，证书发放要用卫士通的 CA；P10 文件选择信安，证书发放要用信安的 CA。

2、证书导入相机。

A、相机证书的导入

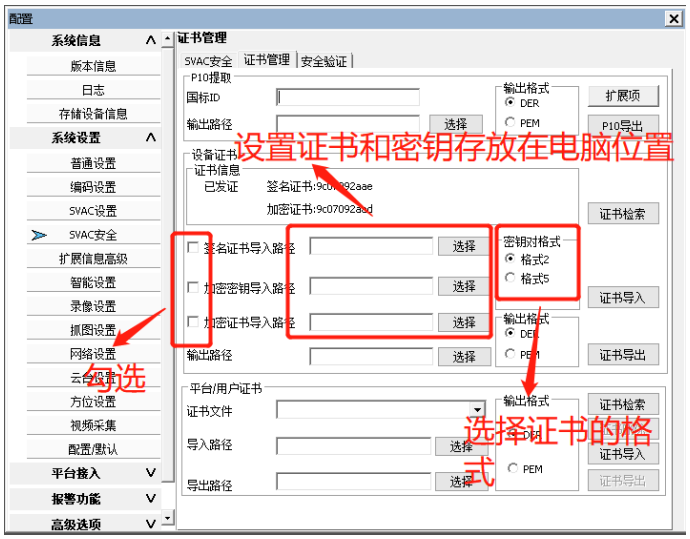
设备证书部分设置和操作以下内容项，如下图：

1）、勾选“签名证书导入路径”、“加密密钥导入路径”、“加密证书导入路径”；

2）、设置证书和密钥的存放路径；

3）、密钥对格式，现在证书和密钥对文件的格式，卫士通选择格式 2，信安选择格式 5。

4）、设置完成后，点击证书导入，即可正常导入相机的证书和密钥到相机。



B、平台（或 SIVS）证书的导入

平台/用户证书部分设置和操作以下内容项，如下图：

1）、设置证书存放路径，双证书需要两个证书在同一目录下；

2）、设置完成后，点击证书导入，即可正常导入平台（或 SIVS）的证书到相机。

注：往相机导入证书时，签名证书的命名有要求，相机只认：国标 ID.cer 。技术人员发的签名证书一般为：国标 ID_SIGN.cer 。请修改名称为：国标 ID.cer 。

加密证书命名不需要修改，保持国标 ID_ENC.cer。

附录三、USBkey 证书的导入

用户 User 国标 ID11-13 位改为 300-399。解码器国标 ID11-13 位改为 114。

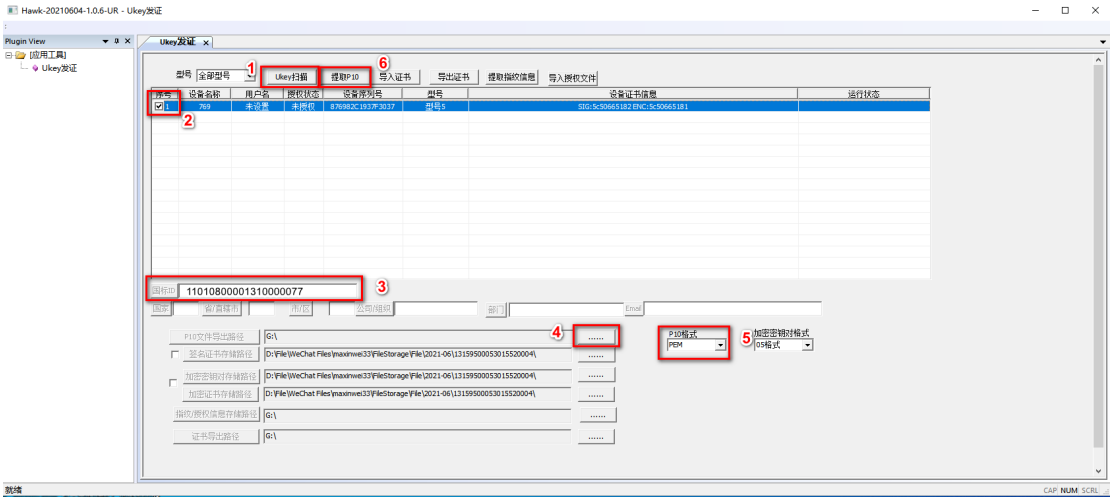
使用 USBkey 发证工具进行操作，具体操作方法如下：

1、准备工作：

1）：USBkey 发证工具联系中星微技术相关人员索要。

2、提取 p10

运行 USBkey 发证工具，具体操作如下：



按照上图红框标记的顺序操作：

1：单击“USBkey 扫描”按钮

2：选中要提取 p10 的 USBkey 设备

3：填写国标 ID

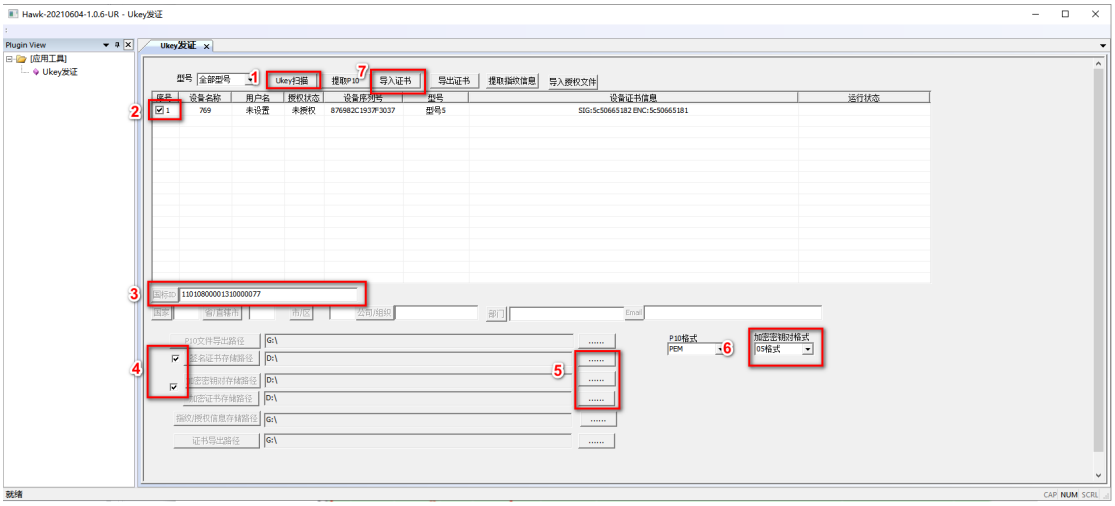
4：指定生成 p10 文件的路径

5：选择 p10 文件的格式，选择 PEM

6：单击“提取 p10”按钮，并输入正确的 USBkey 设备 PIN 码。操作会在指定目录生成 如 11010800001310000077.p10 文件。

信安世纪 USBkey 的 PIN 码缺省 88888888

3、证书导入



按照上图红框标记的顺序操作：

1：单击“USBkey 扫描”按钮

2：选中要导入证书的 USBkey 设备

3：填写要导入证书的国标 ID。相关文件需要符合工具要求，签名证书文件名应为“国标 ID_SIGN.cer”，密钥对文件应为“国标 ID_EncPrivateKey.dat”，加密证书文

件名应为“国标 ID_ENC.cer”。如图中所示相应文件名分别为 11010800001310000077_SIGN.cer, 11010800001310000077_ EncPrivateKey.dat 和 11010800001310000077_ENC.cer

4：如果只需要导入单证，则只勾选“签名证书存储路径”；如果需要导入双证则需同时勾选“签名证书存储路径”和“加密密钥对存储路径”

5：指定相应证书文件所在路径

6：根据实际情况选择“加密密钥对格式”。“05 格式（目前信安使用）”对应“国密 0009 标准”，“raw 格式”对应“国密 0016 标准”

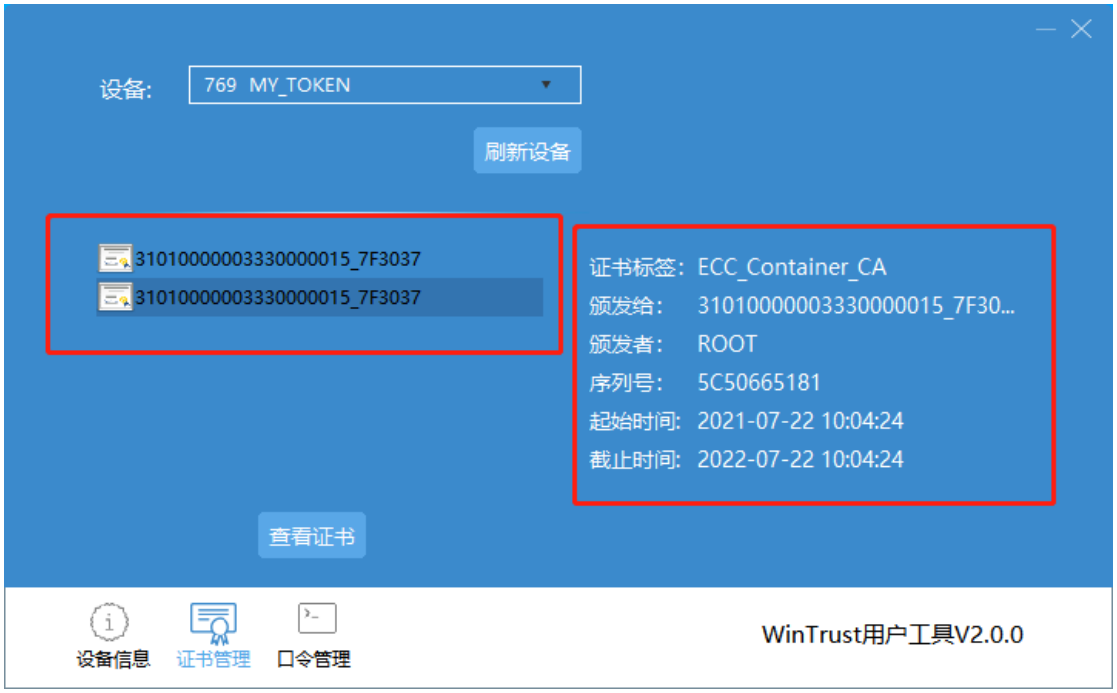
7：单击“导入证书”按钮

附录四、USBkey 证书的验证及导出

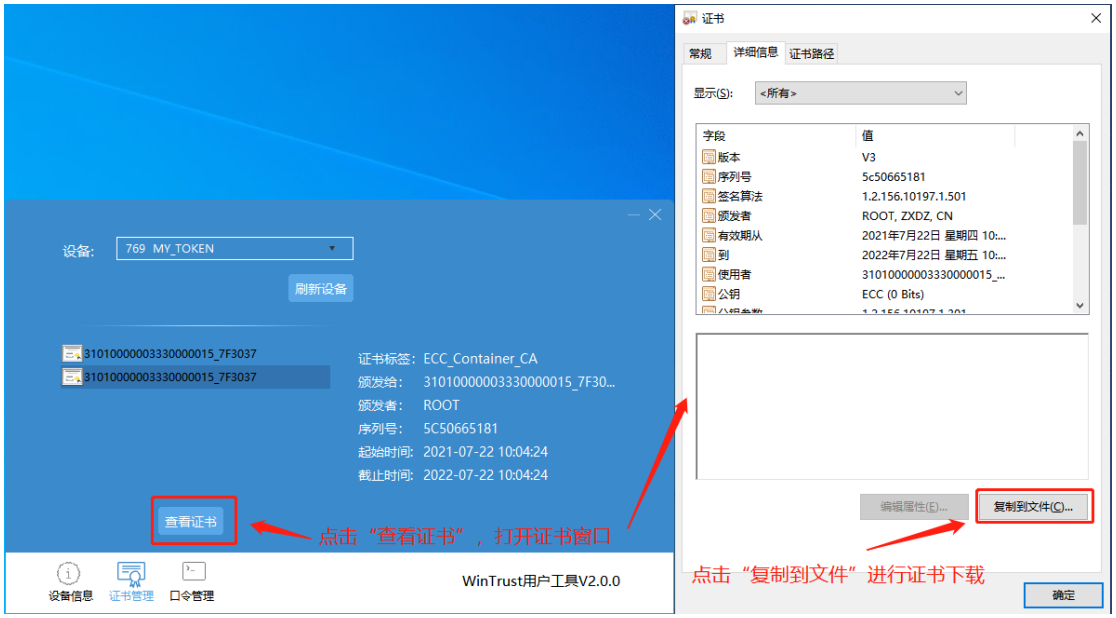
USBkey 用户工具 WinTrust 查看证书

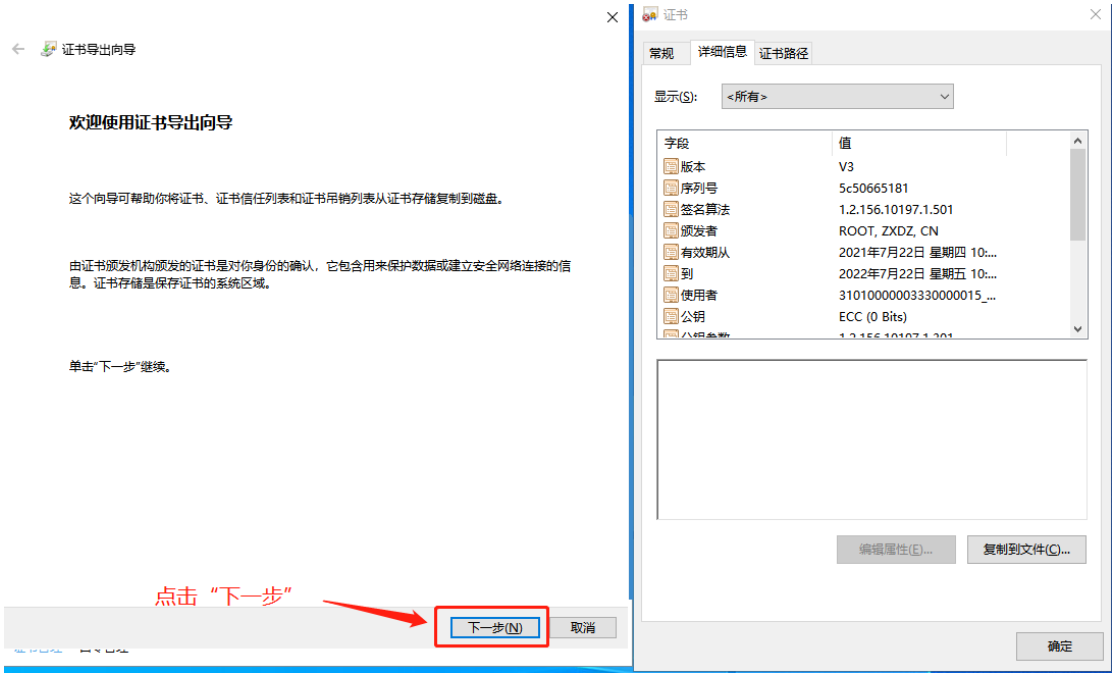
1、将 USBkey 插入到客户端电脑，打开 WinTrust 用户工具，首先查看设备信息确认 USBkey 是否识别成功。

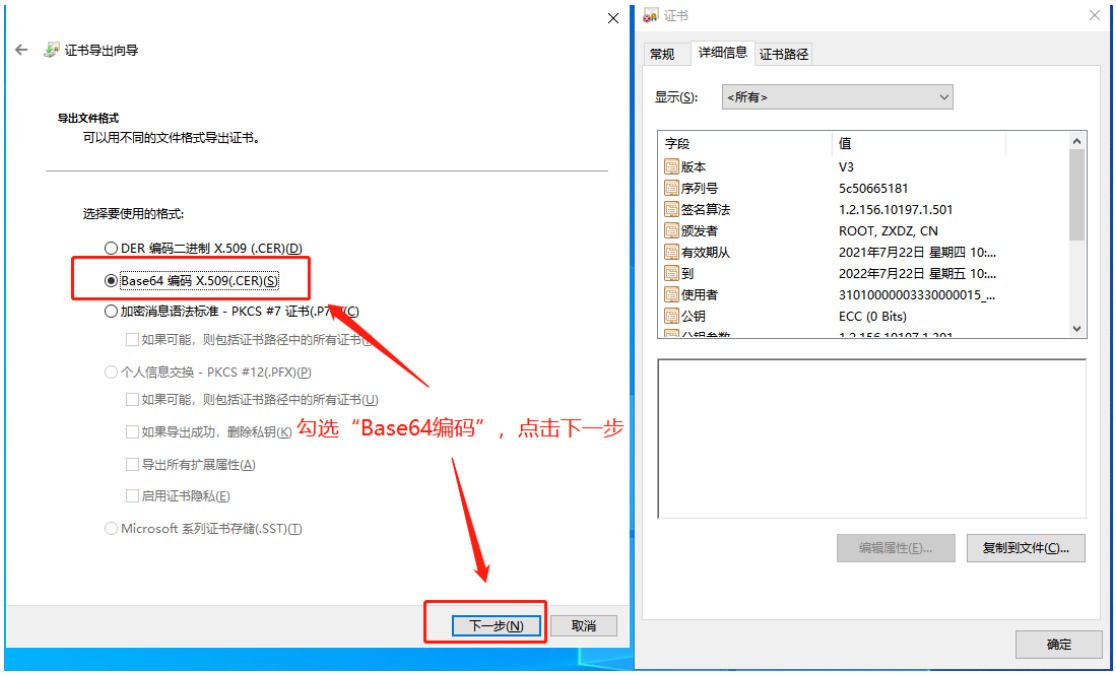
2、点击左下方的“证书管理”，查看证书。

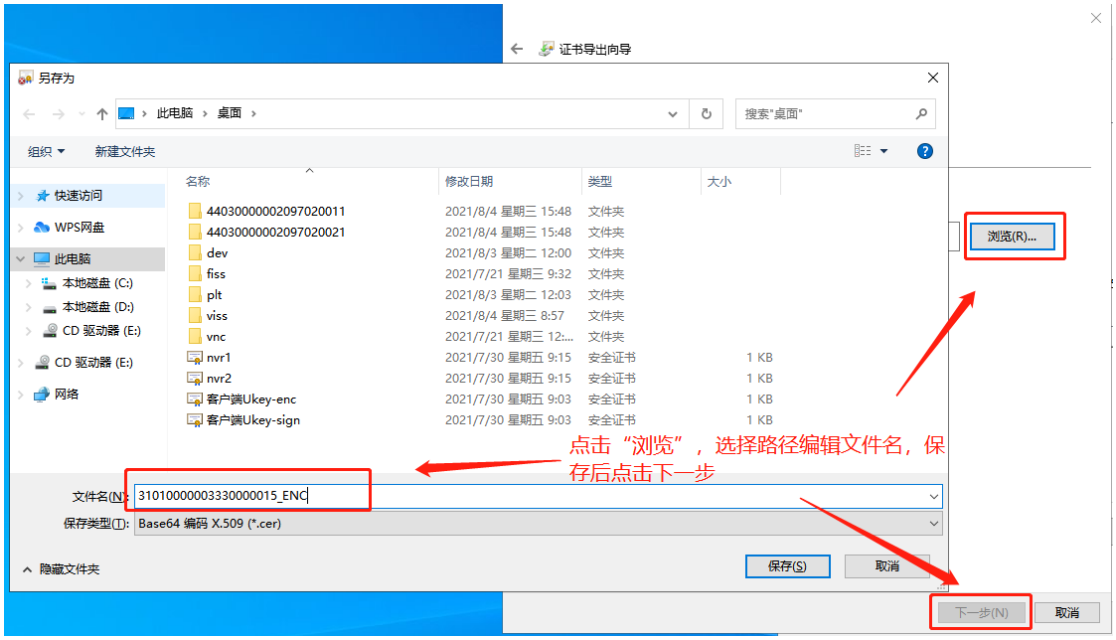


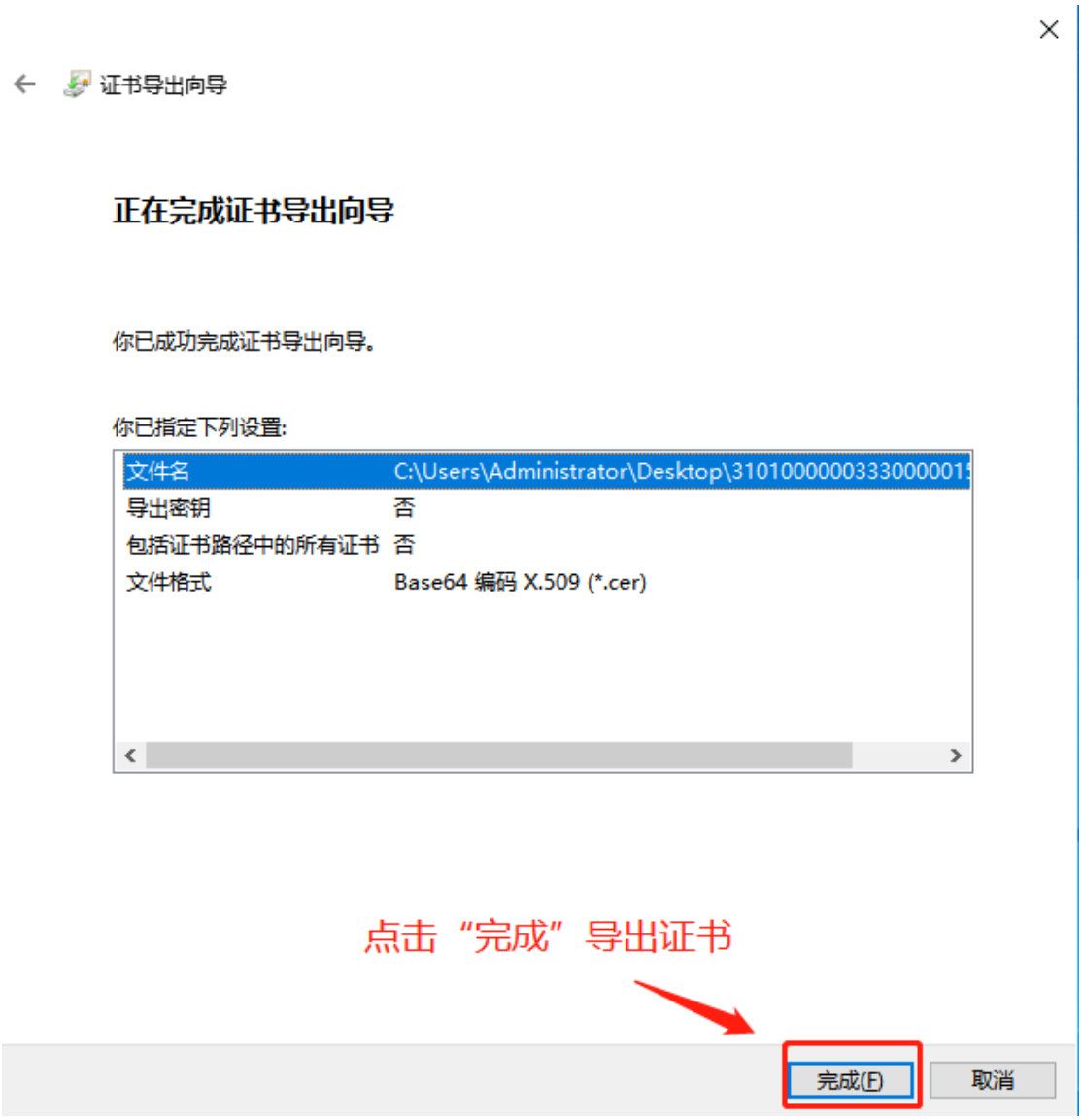
3、现场没有 USBkey 发证工具时，可在证书管理→查看证书，依次将证书导出。（SIVS 新建用户，需导入用户证书，可通过此步骤获取到已下发的用户证书）


设备:
769 MY_TOKEN
刷新设备
3101000000033300000015_7F3037
3101000000033300000015_7F3037
证书标签: ECC_Container_CA
颁发给: 3101000000033300000015_7F30...
颁发者: ROOT
序列号: 5C50665181
起始时间: 2021-07-22 10:04:24
截止时间: 2022-07-22 10:04:24
查看证书
点击“查看证书”，打开证书窗口
设备信息
证书管理
口令管理
WinTrust用户工具V2.0.0
证书
常规
详细信息
证书路径
显示(S):
<所有>
字段
值
版本
V3
序列号
5c50665181
签名算法
1.2.156.10197.1.501
颁发者
ROOT, ZXDZ, CN
有效期从
2021年7月22日 星期四 10:...
到
2022年7月22日 星期五 10:...
使用者
3101000000033300000015_...
公钥
ECC (0 Bits)
编辑属性(E)...
复制到文件(C)...
点击“复制到文件”进行证书下载
确定


证书导出向导
欢迎使用证书导出向导
这个向导可帮助你将证书、证书信任列表和证书吊销列表从证书存储复制到磁盘。
由证书颁发机构颁发的证书是对你身份的确认，它包含用来保护数据或建立安全网络连接的信息。证书存储是保存证书的系统区域。
单击"下一步"继续。
点击“下一步”
下一步(N)
取消
证书
常规
详细信息
证书路径
显示(S):
<所有>
字段
值
版本
V3
序列号
5c50665181
签名算法
1.2.156.10197.1.501
颁发者
ROOT, ZXDZ, CN
有效期从
2021年7月22日 星期四 10:...
到
2022年7月22日 星期五 10:...
使用者
3101000000033300000015_...
公钥
ECC (0 Bits)
编辑属性(E)...
复制到文件(C)...
确定


证书导出向导
导出文件格式
可以用不同的文件格式导出证书。
选择要使用的格式:
DER 编码二进制 X.509 (.CER)(D)
Base64 编码 X.509(.CER)(S)
加密消息语法标准 - PKCS #7 证书(.P7B)(C)
如果可能，则包括证书路径中的所有证书(I)
个人信息交换 - PKCS #12(.PFX)(P)
如果可能，则包括证书路径中的所有证书(U)
如果导出成功，删除私钥(K)
导出所有扩展属性(A)
启用证书隐私(E)
Microsoft 系列证书存储(.SST)(T)
勾选“Base64编码”，点击下一步
下一步(N)
取消
证书
常规
详细信息
证书路径
显示(S):
<所有>
字段
值
版本
V3
序列号
5c50665181
签名算法
1.2.156.10197.1.501
颁发者
ROOT, ZXDZ, CN
有效期从
2021年7月22日 星期四 10:...
到
2022年7月22日 星期五 10:...
使用者
31010000003330000015_...
公钥
ECC (0 Bits)
编辑属性(E)...
复制到文件(C)...
确定


证书导出向导
另存为
此电脑 › 桌面 ›
搜索"桌面"
组织
新建文件夹
快速访问
WPS网盘
此电脑
本地磁盘 (C:)
本地磁盘 (D:)
CD 驱动器 (E:)
CD 驱动器 (E:)
网络
名称
修改日期
类型
大小
44030000002097020011
44030000002097020021
dev
fiss
plt
viss
vnc
nvr1
nvr2
客户端Ukey-enc
客户端Ukey-sign
浏览(R)...
点击“浏览”，选择路径编辑文件名，保存后点击下一步
文件名(N):
31010000003330000015_ENC
保存类型(T):
Base64 编码 X.509 (*.cer)
隐藏文件夹
保存(S)
取消
下一步(N)
取消


证书导出向导
正在完成证书导出向导
你已成功完成证书导出向导。
你已指定下列设置:
文件名 C:\Users\Administrator\Desktop\3101000000333000001
导出密钥 否
包括证书路径中的所有证书 否
文件格式 Base64 编码 X.509 (*.cer)
点击“完成”导出证书
完成(F)
取消

附录五、解码设备配置及证书配置

28181 平台登陆

在桌面快捷键启动 XDCE.exe

；启动后单击右键，如下所示：

点击设置，弹出如下对话框，选择“关系配置”

图中设置结果是，1 号显示器，四分屏画面显示

国标关系配置

国标 ID：VISS 平台解码器上通道号对应的国标 id

屏幕号： 此处从 0 开始计算即显示器编号-1，右键拼接信息查看接入显示器编号

窗口号： 此窗口号从 0 开始算起依次累加，多分屏依次往上加屏幕号不变

关系配置设置完毕后，选择登录配置，如下对话框

平台协议登录信息

服务器 IP 地址：　28181 平台的 IP 地址

服务器类型：　在下拉列表里面选择 28181

服务器端口号：　28181 平台的端口号

本地端口：　本地端口不能被其他程序占用 ，28181 平台注册需要配置

用户名：　28181 平台解码器的设备 id

密码：　28181 平台解码器上配置的密码

电视墙 ID:　随意填

本地 IP 地址：　解码器的机器的本机 IP，28181 平台注册需要配置

点击重新登录成功后登录状态栏里面会变成已登录

国标 28181 安全登陆

如需使用 ukey 或者安全证书登陆国标平台,除正常的登陆配置外,还需如下操作:

国标安全配置信息：

手动编辑解码器运行目录下的 XDCE_Config.xml 文件，(目前暂不支持界面设置)

在 GBSecurityConfig 标签内填写下列字段：

ServerGbId，要登录的国标服务器 ID；

AuthType，登录方式。(0 表示用户名密码登录；1 为软证书安全方式；2 为卫士通 Ukey 安全方式；5 为信安世纪 Ukey 安全方式)；

当 AuthType 设置为 1 时，需要填写下列几项：

SelfSignPrivateKey，xdce 签名私钥文件名及密码；

SelfEncPrivateKey，xdce 加密私钥文件名及密码；

SelfSignPublicKey，xdce 签名公钥文件名；

SelfEncPublicKey，xdce 加密公钥文件名；

OtherSignPublicKey，服务器 gbfg 或 SIVS 的签名公钥；

OtherEncPublicKey，服务器 gbfg 或 SIVS 的加密公钥。

当 AuthType 设置为 2、5 时，需要设置下列几项：

PinCode，默认为 11111111。卫士缺省 11111111 ；信安世纪缺省 88888888

OtherSignPublicKey，服务器 gbfg 或 SIVS 的签名公钥；

OtherEncPublicKey，服务器 gbfg 或 SIVS 的加密公钥。

如果 xdce 选择证书或 Ukey 安全认证登录 ,需要解码器的国标 id 和 ukey 的国标 id 一致，且在国标服务器的解码器上传 ueky 的签名公钥和加密公钥。

附录六、国标 ID 简易介绍

国标 ID 目前使用编码规则 A， 由中心编码(8 位)、行业编码(2 位)、类型编码(3 位)和序号(7 位)四个码段共 20 位十进制数字字符构成。

编码规则 A 的详细说明见表 D.1。其中,中心编码指用户或设备所归属的监控中心的编码,按照监控中心所在地的行政区划代码确定,当不是基层单位时空余位为 0。行政区划代码采用 GB/T2260—2007 规定的行政区划代码表示。行业编码是指用户或设备所归属的行业,行业编码对照表见 D.2。类型编码指定了设备或用户的具体类型,其中的前端设备包含公安系统和非公安系统的前端设备,终端用户包含公安系统和非公安系统的终端用户。

注：以下为常用国标 ID 编码规则。详细编码规则详见《GB/T 28181-2016 安全防范视频监控联网系统信息传输、交换、控制技术要求》中的“附录 D 统一编码规则”。

表 D.1 常用国标 ID 编码规则

<table>
<tr><th>码段</th><th>码位</th><th>含义</th><th colspan="2">取值说明</th></tr>
<tr><td rowspan="4">中心编码</td><td>1、2</td><td>省级编号</td><td colspan="2" rowspan="4">由监控中心所在地的行政区划代码确定,符合 GB/T2260—2007《中华人民共和国行政区划代码》的要求。
1--6 位可简单理解为当地区级行政区身份证前 6 位。第 7、8 位为当地基层接入单位的编码。</td></tr>
<tr><td>3、4</td><td>市级编号</td></tr>
<tr><td>5、6</td><td>区级编号</td></tr>
<tr><td>7、8</td><td>基层接入单位编号</td></tr>
<tr><td>行业编码</td><td>9、10</td><td>行业编码</td><td colspan="2">行业编码对照表见 D.2</td></tr>
<tr><td rowspan="4">类型编码</td><td rowspan="4">11、12、13</td><td rowspan="2">111~130 表示类型为前端主设备</td><td>114</td><td>解码器编码</td></tr>
<tr><td>118</td><td>网络视频录像机(SIVS)编码</td></tr>
<tr><td>131~199 表示类型为前端外围设备</td><td>132</td><td>网络摄像机(IPC)编码</td></tr>
<tr><td></td><td>200</td><td>中心信令控制服务器编码</td></tr>
</table>

		200~299 表示类型为平台设备	203	代理服务器编码
			209	接入网关编码
			211	信令安全路由网关编码
			215	业务分组编码
			216	虚拟组织编码
		300~399 表示类型为中心用户	300	中心用户
			301~343	行业角色用户
网络标识	14	网络标识编码		0、1、2、3、4 为监控报警专网,5 为公安信息网,6 为政务网,7 为 Internet 网,8 为社会资源接入网,9 预留。
序号	15~20	设备、用户序号		

表 D.2 行业编码对照表

接入类型码	名称	建设主体	备注
00	社会治安路面接入	政府机关	包括城市路面、商业街、公共区域、重点区域等
01	社会治安社区接入		包括社区、楼宇、网吧等
02	社会治安内部接入		包括公安办公楼、留置室等
03	社会治安其他接入		
04	交通路面接入		包括城市主要干道、国道、高速交通状况监视
05	交通卡口接入		包括交叉路口、“电子警察”、关口、收费站等
06	交通内部接入		包括交管办公楼等
07	交通其他接入		
08	城市管理接入		
09	卫生环保接入		
10	商检海关接入		
11	教育部门接入		
12~39			预留 1
40	农林牧渔业接入	企业/事业单位	
41	采矿企业接入		
42	制造企业接入		
43	冶金企业接入		
44	电力企业接入		
45	燃气企业接入		
46	建筑企业接入		
47	物流企业接入		
48	邮政企业接入		
49	信息企业接入		
50	住宿和餐饮业接入		
51	金融企业接入		
52	房地产业接入		

53	商务服务业接入		
54	水利企业接入		
55	娱乐企业接入		
56~79			预留 2
80~89		居民自建	预留 3
90~99		其主体	预留 4

附录七、使用注意事项

建议 SIVS 配置 UPS 使用，防止意外断电。

如不能配置 UPS，建议 SIVS 主机增选电池模块，在供电意外断电后，进行正常关机，待供电正常后再行开机。

如有意外断电情况，立即上电后 SIVS 主机不能开机。需切断 SIVS 主机电源 1 分钟，待主板充分放电后，重新上电，这时 SIVS 主机可以正常开机。

拔插多块儿硬盘时，请先关机，以免造成数据丢失。

如需拔掉硬盘，请按顺序将硬盘插回原位置，以免硬盘顺序错乱，导致数据丢失。

SIVS 硬盘安装完成后，尽量不要移动。如需长距离移动，请拆下硬盘。

SIVS 开始录像后，不允许格式化硬盘空间。

浏览和回放 GB35114 安全功能 C 级视频时，请使用已发证的 USBkey。普通用户不能浏览和回放 GB35114 安全功能 C 级视频。

国标 ID 严禁出现重复。

SIVS 主机一定要接地。安装环境要有接地口。

SIVS 的时间，在录像启动后严禁修改。修改时间后，录像会紊乱。建议配置一台 NTP 服务器，每天做校时。