

综合监控一体化平台 用户手册

V2.06

目录

1 产品介绍.....	1
2 登录.....	1
3 基础配置.....	1
3.1 组织管理.....	1
3.2 用户管理.....	3
3.3 人员管理.....	7
3.3.1 基本信息.....	7
3.3.2 房屋信息.....	8
3.3.3 卡片信息.....	8
3.3.4 指纹.....	9
3.3.5 车辆信息.....	10
3.4 设备管理.....	10
3.4.1 普通编码设备.....	10
3.4.2 智能编码设备.....	12
3.4.3 解码设备.....	13
3.4.4 网络键盘.....	14
3.4.5 云端编码设备.....	14
3.4.6 门禁设备.....	15
3.4.7 接入网关.....	16
3.4.8 报警主机.....	17
3.4.9 门禁主机.....	18
3.4.10 安全网关.....	19
3.4.11 出入口设备.....	19
3.4.12 通道.....	20
3.4.13 关联资源.....	22
3.5 服务器管理.....	23
3.5.1 中心服务器.....	23
3.5.2 分布式服务器.....	23
3.5.3 资源重配.....	24
3.6 批量配置.....	25
3.6.1 批量修改密码.....	25
3.6.2 批量码流加扰.....	25
3.6.3 NVR批量操作.....	25
3.6.4 批量编码参数配置.....	26
3.6.5 设备升级.....	27
3.7 录像计划.....	27
3.7.1 时间模板.....	27
3.7.2 录像计划.....	29

3.8 流分发管理.....	30
3.8.1 私有协议.....	30
3.8.2 RTMP.....	31
4 报警配置.....	31
4.1 报警配置.....	31
4.2 时间模板.....	34
4.3 邮件记录.....	34
4.4 报警级别自定义.....	34
4.5 报警订阅.....	35
4.5.1 客户端报警订阅.....	35
4.5.2 设备报警订阅.....	36
4.6 报警自定义.....	39
4.6.1 报警自定义.....	39
4.6.2 通用报警.....	40
5 录像备份.....	41
5.1 自动备份.....	41
5.2 本地备份.....	42
6 系统配置.....	43
6.1 基本配置.....	43
6.1.1 基本配置.....	43
6.1.2 时间配置.....	44
6.1.3 时间同步.....	44
6.1.4 假日配置.....	45
6.1.5 图像矫正.....	45
6.2 硬盘配置.....	45
6.2.1 阵列配置.....	46
6.2.2 硬盘管理.....	47
6.2.3 网络硬盘.....	47
6.2.4 容量配置.....	48
6.2.5 盘组属性.....	49
6.2.6 高级配置.....	49
6.3 网络配置.....	50
6.3.1 TCP/IP.....	50
6.3.2 宇视云.....	51
6.3.3 DDNS.....	52
6.3.4 端口.....	52
6.3.5 端口映射.....	52
6.3.6 自定义路由.....	53
6.3.7 邮件.....	53
6.3.8 AD域配置.....	53

6.4 协议对接.....	54
6.4.1 UNP.....	54
6.4.2 国标.....	56
6.4.3 视图库.....	57
6.4.4 监管平台.....	59
6.5 安全配置.....	60
6.5.1 802.1x.....	60
6.5.2 ARP攻击.....	60
6.5.3 HTTPS.....	61
6.5.4 SSH.....	61
6.5.5 IP地址过滤.....	61
6.6 系统维护.....	62
6.6.1 系统维护.....	62
6.6.2 设备诊断信息.....	62
6.6.3 日志清理.....	63
6.6.4 网络抓包.....	63
6.6.5 网络检测.....	64
6.6.6 网络资源统计.....	64
6.6.7 媒体流传输策略.....	64
6.6.8 数据备份.....	65
6.6.9 一键收集.....	66
6.7 主从切换.....	66
6.7.1 主机切换为从机.....	66
6.7.2 从机切换为主机.....	67
6.7.3 更换主机.....	67
6.7.4 热备配置.....	67
6.8 地图配置.....	68
6.9 组件管理.....	68
7 视频应用.....	68
7.1 实况.....	68
7.2 回放.....	70
7.3 录像下载.....	72
7.4 本地配置.....	74
8 运维统计.....	75
8.1 服务器统计.....	75
8.1.1 服务器状态.....	75
8.1.2 硬盘检测.....	75
8.1.3 网络状态.....	76
8.1.4 在线用户.....	76
8.1.5 带宽统计.....	76

8.1.6	丢包率统计	77
8.1.7	服务器性能	77
8.1.8	存储能力	78
8.1.9	录像状态	79
8.2	设备统计	80
8.3	日志查询	81
8.3.1	服务器报警日志	81
8.3.2	设备报警日志	81
8.3.3	操作日志	81
9	门禁管理	82
9.1	权限管理	82
9.1.1	时间模板	82
9.1.2	门组	82
9.1.3	门禁授权	83
9.1.4	核验模板	85
9.2	门卡管理	85
9.3	小区管理	86
9.3.1	添加房屋	86
9.3.2	入住人员管理	87
9.4	考勤管理	88
9.4.1	考勤制度	88
9.4.2	人员排班	88
9.4.3	考勤处理	93
9.4.4	考勤统计	94
10	平台直连公网的端口映射配置指导	96
10.1	准备	96
10.2	路由器配置	96
10.3	平台配置	98
11	RTSP协议接入设备	101
12	自定义多源数据融幕	102
12.1	数据图表	104

1 产品介绍

综合监控一体化平台（以下简称平台、平台服务器或服务器）是针对中小型视频监控解决方案而设计研发的新一代专业视频管理操作设备。平台支持通过以下三种方式登录并进行相应的配置与操作：

登录方式	介绍
网页客户端	通过Web浏览器登录平台进行设备、业务等的管理、配置、维护操作；支持简单的视频业务。
软件客户端	通过安装客户端软件登录平台进行各种业务操作。
手机客户端	通过手机客户端登录平台进行简单的实况、回放和设备管理操作。

本手册介绍网页客户端的操作使用。若无特殊说明，手册中的“平台”均指综合监控一体化平台。设备，指平台管理的下行设备，如IPC、NVR等。

2 登录

通过网页客户端登录平台：

- 打开浏览器，在地址栏中输入平台的IP地址，如192.168.1.60。
- 输入用户名和密码登录。默认用户名/密码：admin/123456。



说明：

若系统已配置AD域并导入域用户，可通过已导入的域用户名/密码登录。

- 登录后建议修改密码。



重要：

- 为确保安全，请在首次登录时修改为强密码，9-32位密码且包含以下三种：大小写字母、特殊字符、阿拉伯数字。
- 首次登录admin用户可设置联系方式，用于密码找回。若暂不输入或需要修改，之后可在用户单击 输入/修改联系方式。
- 如果忘记密码，可点击<登录>按钮上方的<忘记密码>，然后根据提示，获取临时密码后登录。临时密码只用于局域网和admin用户，只在当天有效。登录后请修改密码。

3 基础配置

基础配置是对人员、用户、组织、设备、服务器、流分发、录像计划进行统一添加、管理或进行批量配置。通过基础配置可对平台上的人员、登录用户、组织、设备等基础信息进行添加、管理，方便在业务应用中使用。

支持组织管理、用户管理、人员管理、设备管理、录像计划、批量配置、服务器管理和流分发管理。

3.1 组织管理

新建组织，以便将平台下的资源（如设备和通道）划归到不同组织中管理。组织以树状结构的形式进行管理，因此称为组织树。系统初始化时生成一个根组织（root），用户在此基础上新建其他组织。

基本组织

一台设备（如IPC或NVR）只能属于一个基本组织；一台NVR下的所有IPC只能属于同一个基本组织。

基础配置>组织管理>基本组织

1. 点击<添加>新建基本组织。
2. 输入组织名称并选择上级组织（默认为根组织）。
3. 点击<确定>。
4. 新组织出现在左侧组织树、右侧组织列表中，同时出现在添加设备时[组织名称]下拉列表中。添加设备时可选。
5. 在组织列表中，可点击  编辑组织，或点击  删除组织。



说明:

不能删除根组织或包含下级组织、设备或通道的组织。

自定义组织

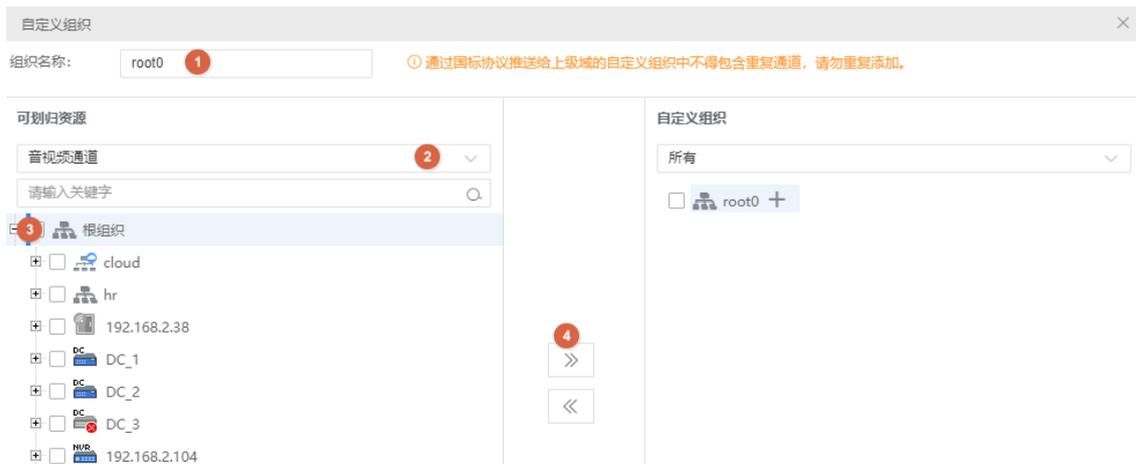
自定义组织提供更为灵活的管理方式。

基础配置>组织管理>自定义组织

自定义组织提供了一种更为灵活的管理方式，支持：

- 将一台NVR下的摄像机划归到不同组织中管理
- 将不同NVR下的摄像机划归到同一个组织中管理
- 将一台摄像机同时划归到多个组织
- 将自定义组织分配给指定角色，使用户在软件客户端上只能操作特定的资源
- 将各种类型的资源（如音视频通道）划归给不同组织管理

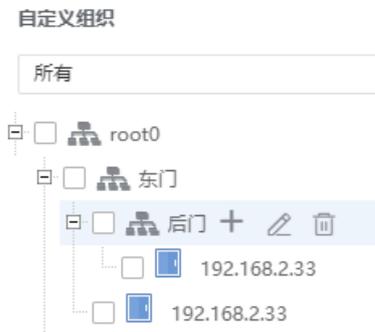
1. 点击<添加>新建自定义组织：
2. 输入组织名称。组织名自动更新在右侧。



3. （可选）选择要划归的资源类型（如音视频通道）。可输入关键字过滤。
4. 若要划归到根组织（如园区），在右侧点击选择组织，在左侧选择资源，然后点击<添加>。
5. 若要新建下级组织，点击根组织右侧的添加符号，输入组织名。组织树自动更新。可用同样的方法继续添加下级组织。可编辑或删除已添加的组织。

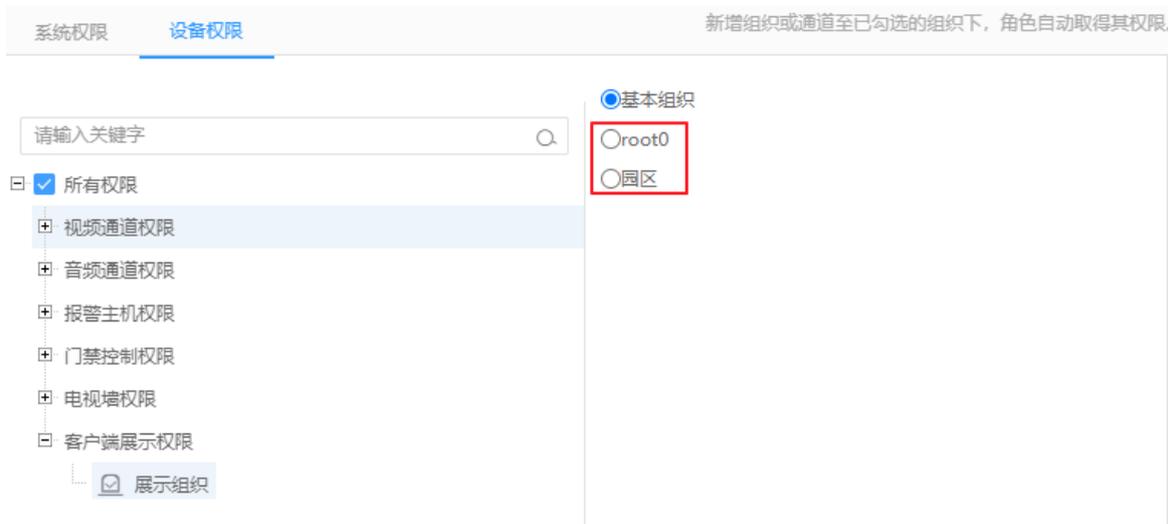


6. 在右侧点击选择组织，在左侧勾选资源，然后点击<添加>，将资源划归到目标组织中。同一个资源可同时划归到不同组织（如下图所示）。



7. 点击<确定>。

新建组织的根组织（如园区）出现在添加或修改角色对话框的[设备权限]页签下。通过将角色与该组织绑定，使拥有该角色的用户可以在软件客户端上访问该组织下的资源（如园区下的音视频通道）。



说明:

- 系统权限分为操作端权限（软件客户端）和管理端权限。操作端权限是展示组织与权限配置的交集。
- 对于拥有多个角色的用户，不同角色所绑定的自定义组织同时展示在软件客户端的实况、回放、轮巡、视图、语音、电视墙、客流量统计等模块的资源列表中。

3.2 用户管理

配置角色并为角色分配权限；通过分配角色来控制用户权限。可以将一个角色分配给多个用户，一个用户最多拥有16个角色。

角色

基础配置>用户管理>角色

角色包括：

- 系统权限：分为操作端（软件客户端）权限、管理端（网页客户端）权限，对角色各项操作和管理模块的权限进行设定。比如，向一个角色只分配预览（实况和回放）权限，如果一个用户只有这个角色，那么该用户登录软件客户端后将只能看到实况、回放和报警记录三个常用功能模块。
- 设备权限：对操作设备时可使用的功能进行权限设定。设置时，除了要选择权限外，还需要指定组织或通道。
- 角色等级：主要用于区分含有相同权限的角色在操作摄像机云台时的优先级。

1. 点击<添加>新建角色。
2. 输入角色名称。
3. 选择角色等级。

4. (可选) 利用现有角色进行快速配置: 勾选[复制角色], 从右侧下拉框中选择一个角色。该角色的权限自动展现在界面上。可以以此为基础进行快速编辑。选中角色的权限不会被改变。

添加角色

* 角色名称: 复制角色

* 角色等级:

5. 在[系统权限]页签下, 选择要分配的系统权限。比如, 如果只允许查看实况和录像的权限, 那么只勾选[操作端权限]下的[预览]。勾选[预览]后, [实况]和[回放]将自动被勾选。

系统权限 设备权限

系统权限

请输入关键字

所有权限

- 操作端权限
- 管理端权限

6. 点击[设备权限]页签, 选择权限并相应地选择组织通道。

系统权限 设备权限 新增组织或通道至已勾选的组织下, 角色自动取得其权限。

设备权限

请输入关键字

所有权限

- 视频通道权限
- 音频通道权限
- 报警主机权限
- 门禁控制权限
- 电视墙权限
- 客户端展示权限

组织通道

- 根组织
- hr
- cloud
- 192.168.2.30_V_1
- 192.168.2.30_V_2
- 192.168.2.30_V_3
- 192.168.2.30_V_4
- 192.168.2.30_V_5
- 192.168.2.30_V_6
- 192.168.2.104_V_01
- 192.168.2.104_V_02
- 192.168.2.104_V_03
- 192.168.2.104_V_04

 说明:

- 在左侧点击权限 (如[实时预览]) 后, 需在右侧勾选组织和通道, 表示该角色拥有选中组织通道的实时预览权限。
- 勾选[所有权限]将自动勾选所有权限和所有通道。勾选[根组织]将自动勾选所有通道。
- 点击  可从选中节点 (如[实时预览]) 复制权限至当前节点 (如[录像回放])。比如, 为[实时预览]勾选完组织通道后, 如果要为[录像回放]选择相同的通道, 可以先点击[实时预览], 然后点击[录像回放]右侧的  图标, 将为[录像回放]自动勾选相同的组织通道, 免去重复操作。
- 权限左侧的 符号表示已经选择过组织通道。
- 点击[客户端展示权限]节点下的[展示组织], 右侧将出现基本组织和已创建的自定义组织 (根组织)。可根据需要选择一个组织。更多信息, 请见[自定义组织](#)。

- (可选) 在备注栏中输入备注信息，如角色描述。
- 完成设置后，点击<确定>。
- 创建完的角色出现在角色列表中。

<input type="checkbox"/>	角色	角色等级	客户端显示组织	操作
<input type="checkbox"/>	All	最高	基本组织	
<input type="checkbox"/>	Manager	最高	基本组织	
<input type="checkbox"/>	Operator	最高	基本组织	



说明:

- 点击 编辑角色。相应权限变动将自动同步至拥有该角色的用户。
- 点击 删除角色。删除角色后，该角色下用户的相应权限也会被同步删除。
- 用户权限变更后，已经登录的用户将被登出，需重新登录。

用户

基础配置>用户管理>用户

添加、编辑、删除用户。用户可以登录平台，通过为用户分配不同的角色来限定用户的配置和操作权限，以实现权限的管理。可以锁定用户，限制其登录。



说明:

系统管理员 (admin) 不能被删除或锁定。

支持添加用户或导入域用户。

- 添加用户：
 - 单击<添加>创建用户。

添加
×

* 用户名:

角色:

* 密码:

弱 中 强

* 确认密码:

有效日期: -

时间模板:

建议修改为强密码 (至少9位,且包含以下三种: 大小写字母、特殊字符、阿拉伯数字)。

选填

确定

取消

- 根据以下说明配置用户。

- 用户名：必须唯一，设定后不能修改。
- 角色：每个用户最多可分配16个角色。用户拥有所有角色的权限集合。
- 密码：用户登录平台客户端的密码。
- 有效日期：账户的有效日期。用户在有效期之外不能登录。
- 时间模板：见[用户时间模板](#)。
- 可点击展开配置更多信息。

3. 单击<确定>完成添加。

- 导入域用户：当系统已加入AD域时，可导入域用户，导入的域用户可使用其域用户名/密码登录该服务器。单击[[更多链接](#)>AD域配置]可快速跳转配置。

1. 单击<导入域用户>弹出导入窗口。

2. 在左侧域服务器组织上选择需要导入的域用户，单击添加到列表。

3. 设置用户状态和权限。

- 用户状态：正常状态可登录系统，锁定则无法登录。
- 角色：每个用户最多可分配16个角色。用户拥有所有角色的权限集合。
- 有效日期：账户的有效日期。用户在有效期之外不能登录。
- 时间模板：见[用户时间模板](#)。

4. 单击<确定>完成导入。

使用操作栏中的按钮对用户进行管理：

- 点击修改用户角色、有效日期、时间模板等信息，admin用户仅可修改联系方式。
- 点击修改密码。新密码在下次登录时生效。只有超级管理员（admin）有权修改其他用户的密码。
- 点击锁定用户。被锁定的用户在解锁前无法登录。
- 点击删除用户。已登录的用户将被强制退出。
- 单击<同步域用户信息>可将系统中的域用户信息更新为域控制服务器上最新用户信息，仅完成AD域配置的服务器可进行此操作。

用户时间模板

基础配置>用户管理>用户时间模板

通过用户时间模板限制用户的登录时间。需要先配置用户时间模板，然后在添加或编辑用户时选择该时间模板。用户只能在时间模板中设定的时间内登录客户端。

说明:

- 系统自带All-day模板，可以编辑，不能删除。被分配All-day模板的用户没有登录时间限制。
- 每天最多允许设置8个时段。

添加时间模板
✕

模板名称:

复制模板

编辑
 重置

每天最多可设置8个时段

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
星期日																									
星期一																									
星期二																									
星期三																									
星期四																									
星期五																									
星期六																									
假日																									

假日说明: 配置假日前请先启用假日日期, 否则配置不生效。

4 擦除

3 ■ 有效时间

备注:

确定
取消

编号	说明
1	输入模板名称 (必须唯一)。
2	勾选后, 可选择一个已有模板, 在该模板基础上修改编辑。
3	点击后, 在左侧点击或拖动鼠标绘制时间段。横轴表示0-24点。紫色表示允许登录时段; 白色表示禁止登录时段。
4	点击后, 在左侧点击或拖动鼠标, 删除允许登录时段。
5	点击精确设置时间段。可使用“复制到”功能, 将某天的设置复制给其他天 (先勾选, 再点击<复制>)。
6	点击清除所有时间段。

3.3 人员管理

添加人员, 用于房屋住户管理、门禁核验等。

首次添加人员时需安装WebAssist插件, 安装完后请重新登录。

3.3.1 基本信息

录入人员基本信息。

采集:	<input type="text"/>	...	确定
*人员编号:	<input type="text"/>	出生年月:	<input type="text" value="2021/03/04"/>
*姓名:	<input type="text"/>	手机号码:	<input type="text"/>
性别:	<input checked="" type="radio"/> 男 <input type="radio"/> 女 <input type="radio"/> 未知	所属部门:	<input type="text" value="dept"/>
证件类型:	<input type="text" value="身份证"/>	地址:	<input type="text"/>
*证件号码:	<input type="text"/>		

员工照片: (建议上传数量不超过6张, 大小为10-500KB、分辨率不超过1672*1080的.jpg格式图片)

[图像矫正](#)



添加照片

3.3.2 房屋信息

选择业主或租客，并设置房屋信息。以下以业主为例，租客还需设置租期。可选房屋在[小区管理](#)中配置。点击<添加>或<删除>按钮添加或删除房屋。

*住户类型:	<input type="text" value="业主"/>							
+ 添加								
*小区:	<input type="text" value="智慧小"/>	*楼栋:	<input type="text" value="智慧小"/>	*房间号:	<input type="text" value="智慧小区"/>	*是否产权人:	<input type="text" value="一手"/>	<input type="button" value="X"/>

3.3.3 卡片信息

为人员指定门禁卡，设置卡片密码和有效期。可手动选择卡号或使用发卡器读取卡号。

若手动选择卡号，需先在[门禁管理>门卡管理>空白卡]中新增卡号。注意选择完卡号后需点击<确定>。若使用发卡器，点击<发卡器配置>，选择卡片类型，然后点击<开始读取>，用发卡器自动读取卡号写入平台。

卡片密码:

有效时间: 截止时间:

发卡模式: 手动选择 ...

发卡器

① 修改卡密码或有效期后需重新授权才生效。

卡号	卡片类型	卡状态	生效时间	截止时间
暂无数据				

3.3.4 指纹

支持录入人员指纹（用于门禁核验）。每人最多可录入10个指纹。

+ 录入指纹

	指纹名称	操作
❏		

录入指纹
×

①
 环境准备

②
 录入指纹

③
 完成

1、请录入指纹



将手指平放在传感器上，请确保手指和传感器清洁。

1. 客户端电脑需连接好指纹录入设备。
2. 点击<录入指纹>，根据提示完成指纹录入。

后续操作

如需在门禁上使用指纹核验开门，还需配置门禁设备。

1. 在[门禁管理-权限管理-[核验模板](#)]界面，添加核验模板，选择核验方式为“指纹白名单”。
2. 在[基础配置-设备管理-通道-[门禁通道](#)]界面，对支持指纹核验的门禁设备配置“1：N相似阈值”、“人员库”、“核验模板”。

3.3.5 车辆信息

添加人员所拥有的车辆信息。每人最多可添加16辆车。

+ 添加
🗑️ 删除

	基本信息	操作
<input type="checkbox"/>	<div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;">111245</div> <div style="margin-right: 10px;">111</div> <div style="font-size: 0.8em;">🚗 小型车</div> </div>	✎ 🗑️

添加
×

车辆信息

* 车牌号码: +

车牌类型:

车牌颜色:

车辆类型:

车辆颜色:

图片大小不超过1M

上传图片

注意：每人最多可添加16辆车。

完成
取消

3.4 设备管理

3.4.1 普通编码设备

基础配置>设备管理>设备>普通编码设备

普通编码设备包括IPC（网络摄像机，简称摄像机或相机）、NVR（网络视频录像机）和编码器。

说明:

UNP设备不支持录像计划配置。添加编码设备时，请前往[系统配置>协议对接>UNP>UNP服务器]查看“UNP服务器”是否开启。如果开启，且编码设备的IP地址在“UNP客户端虚拟地址池”范围内，那么该编码设备将被添加为UNP设备，不能配置录像计划。更多信息，请见[UNP](#)。

说明:

- 点击<精确添加>，添加一台已知IP地址/域名的设备。
- 若要以RTSP协议接入IPC或NVR查看实况，点击<精确添加>，然后从[接入协议]下拉框选择“自定义”。具体操作请见[RTSP协议接入设备](#)。

支持精确添加、批量添加和自动搜索三种方式添加设备。

- 精确添加：添加一台已知IP地址/域名的设备
 1. 点击<精确添加>弹出[添加设备]框。
 2. 输入设备信息，点击<确定>完成添加。
- 批量添加：在模板中填写设备信息，批量导入至平台。
 1. 点击页面上方的<批量添加/修改>，弹出[导入]框。
 2. 点击<下载导入模板>，在下载的模板中填写设备信息。
 3. 点击  选择需要上传的文件，点击<确定>完成导入。
- 自动搜索：自动搜索添加与平台同网段的设备。
 1. 点击<自动搜索>，发现与平台同网段的编码设备。



管理状态	IP地址	端口	设备类型	设备型号	序列号	所属服务器	操作
<input type="checkbox"/> 未添加	192.168.2.71	80	IPC			VMS	+
<input type="checkbox"/> 未添加	192.168.2.223	80	IPC			VMS	+
<input type="checkbox"/> 未添加	192.168.2.250	80	IPC			VMS	+

说明:

NVR设备不支持以ONVIF协议接入。

2. 要添加单台设备，点击对应+。要批量添加配置（服务器、协议类型、组织、用户名/密码）相同的设备，勾选设备，点击<批量添加>。
3. 可设置条件重新搜索：
 - 所属服务器：主从配置下可选，选择进行设备搜索的服务器。
 - 若配置了UNP，可选择[UNP设备]单选框，搜索指定所属服务器下的UNP设备并添加到该服务器上。
 - IP地址：搜索指定地址范围内的普通设备（非UNP设备）。
 - 根据管理状态（是否已添加）和设备类型过滤。
 - 点击[国标搜索]页签，只搜索国标设备。需先完成平台及下行设备的国标配置（见[国标服务器配置](#)和[国标本地配置](#)）。
4. 完成添加后，查看设备在线状态。

说明:

如果在线状态显示“离线-用户名或密码错误”，请点击  修改密码；否则设备无法上线。

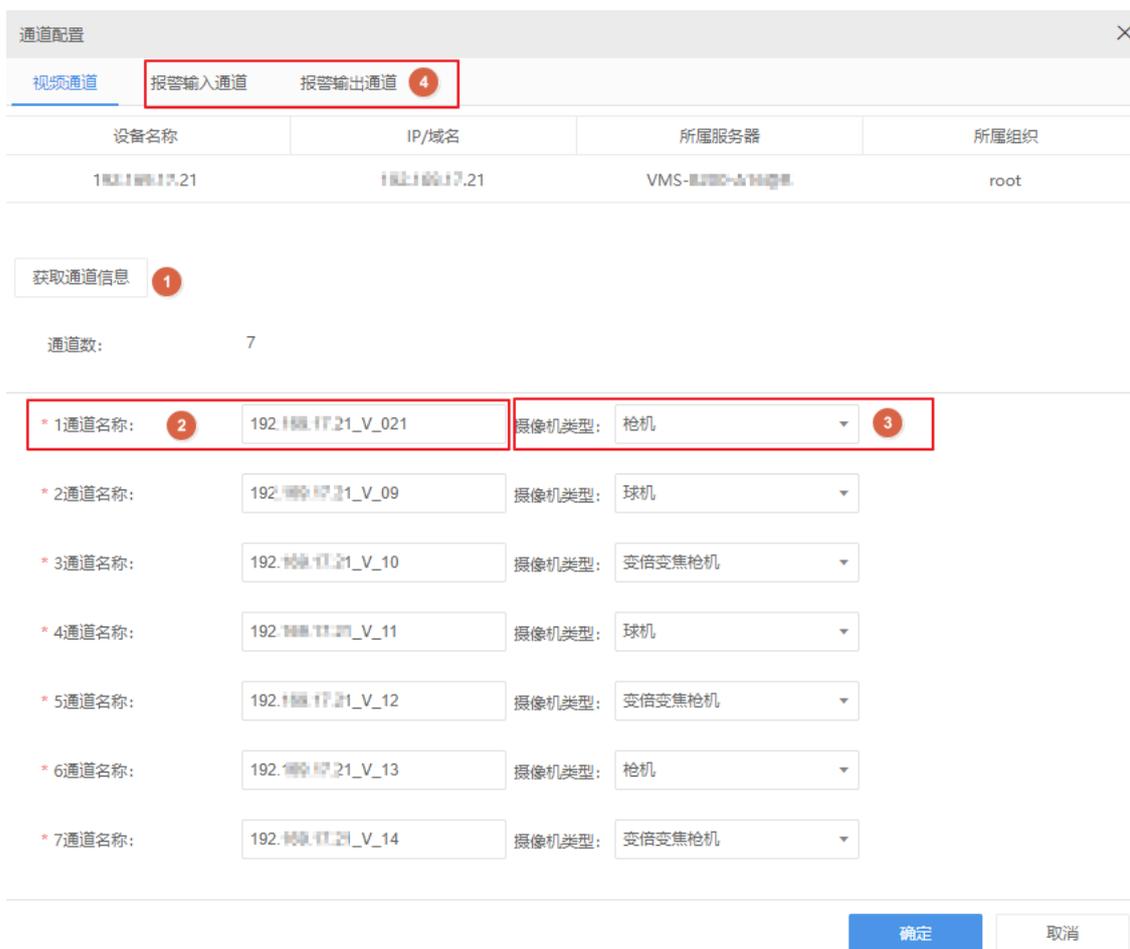
其他操作

- 导出：单击页面上方的<导出>可导出设备列表。
- 编辑：单击设备操作列下的  或批量勾选设备后单击上方的<编辑>修改设备信息。

说明:

如需将设备添加至从机，可修改设备所属服务器为从机。

- 批量修改：在导出的设备列表中，修改设备信息。然后单击<批量添加/修改>，导入修改后的表格即可。
- 删除：单击设备操作列下的或批量勾选设备后单击上方的<删除>删除设备。
- 获取通道信息：单击设备操作列下的按钮，打开窗口如下图所示。
 - (1) 获取该设备的通道信息。
 - (2) 修改平台上的通道名称，修改通道名称不会修改保存在该设备上的通道名称。
 - (3) 选择通道摄像机类型，不同摄像机类型在资源树中显示的图标不同：枪机，球机，变倍变焦枪机。
 - (4) 查看该设备的报警输入通道和报警输出通道。



- 访问设备Web页面：单击设备操作列下的可跳转设备Web页面。
- 同步通道信息：勾选设备后单击上方的<同步通道信息>可批量将多台设备的通道信息同步至平台。在[基础配置>设备管理>通道>编码通道]下查看同步后的通道信息。

3.4.2 智能编码设备

基础配置>设备管理>设备>智能编码设备

添加智能编码设备(IPC/NVR/AIBox/EIA)，实现人脸识别、卡口监控、混行检测等功能。

人脸识别和卡口监控

添加用于人脸识别和卡口监控的智能设备。完成后，可在软件客户端上操作“人脸识别”和“卡口监控”模块。

1. 添加设备具体操作步骤请参见[普通编码设备](#)。



说明:

关于设置“图片协议”：

- 添加卡口相机或NVR时请选择“视图库”。设备侧需完成视图库相关配置（见[视图库](#)），包括服务器地址（平台的IP地址）、服务器端口（5073）、平台通信类型（GA/T1400）和接入用户名/密码。
- 添加人脸识别相机时，对第三方相机请选择“视图库”；对我司相机请选择“私有”或“视图库”。“视图库”协议支持人脸图片的抓拍上报；“私有”协议支持更多功能（如人脸布控、匹配/不匹配告警上报、结构化数据上报等）。

2. 查看设备状态是否为“在线”；以视图库协议添加的设备，若注册成功，其视图库状态显示为“已注册”。

设备名称	IP地址	设备类型	接入协议	图片协议	所属服务器	所属组织	设备型号	视图库状态	在线状态	操作
192.168.1.25	192.168.1.25	Alibox	私有	私有	VMS-8200-ALIBOX	root	AOX-0313000-D	--	在线	编辑 删除 刷新
192.168.1.25	192.168.1.25	NVR	私有	私有	VMS-8200-ALIBOX	root	NVR-8200-ALIBOX-IQ	--	在线	编辑 删除 刷新

混行检测

添加支持混行检测的智能设备。完成添加后，可在软件客户端上操作“混行检测”模块。

1. 先在相机Web界面完成所需配置，包括开启混行检测、勾选抓拍目标（机动车、非机动车或行人）等。具体请参见《混行检测工勘指导书》。
2. 点击<自动搜索>或<精确添加>按钮添加设备（具体操作步骤请参见[普通编码设备](#)）。



说明:

添加时选择“私有”图片协议。

点击页面上方的<导出>可导出设备列表。

3.4.3 解码设备

基础配置>设备管理>设备>解码设备

解码设备包括内置解码器（设备自带）、解码卡（选购）、外置解码器、拼接控制器。



说明:

- 支持的解码设备因平台型号而异。比如仅特定型号自带内置解码器或支持解码卡。具体以平台实际功能为准。
- 精确添加和批量导入具体操作步骤请参见[普通编码设备](#)。

1. 点击<自动搜索>，搜索与平台同网段的解码设备。

管理状态	IP地址	端口	设备类型	设备型号	序列号	所属服务器	操作
已添加	192.168.2.50	80	其他	EDU		VMS	
已添加	192.168.2.38	80	其他	EDU		VMS	
未添加	192.168.2.187	80	其他	IPC		VMS	+
未添加	192.168.2.252	80	其他	IPC		VMS	+

2. 要添加某台设备，点击对应。对配置（协议、组织、用户名/密码）相同的设备，勾选设备后点击<批量添加>。
3. 可设置条件重新搜索：
 - IP地址：搜索指定地址范围内设备。
 - 根据管理状态（是否添加）和设备类型（解码器/拼接控制器）过滤。
4. 完成添加后，查看设备在线状态。

说明:

- 如果在线状态显示“离线-用户名或密码错误”，请点击  修改密码；否则设备无法上线。
- 若安装了解码卡，则DC_2或DC_3在线。DC_2对应槽位SLOT0的解码卡；DC_3对应槽位SLOT1的解码卡，未安装解码卡则不显示DC_2、DC_3。可点击  修改设备名称。

点击页面上方的<导出>可导出设备列表。

3.4.4 网络键盘

基础配置>设备管理>设备>网络键盘

添加网络键盘，在电视墙上实现视频上墙、分屏、窗口放大/缩小、云台控制等操作。

说明:

先参照《网络键盘手册》完成键盘基本配置，包括在键盘上输入平台的IP地址和端口号，完成键盘向平台的注册。然后按照以下操作，设置需要通过键盘控制的视频通道、解码通道或电视墙。

1. 添加需要通过键盘控制的视频通道（相机）。每个视频通道自动被分配一个通道编号（如1）。



通道编号	解码通道名称	所属组织	码流类型	状态	操作
1	192.168.2.100_V_01	root	主码流	在线	 

2. 若键盘配合解码器电视墙或解码卡电视墙使用，在[解码通道列表]页签下添加解码通道。每个解码通道自动被分配一个通道编号（如1、2、3）。



通道编号	解码通道名称	所属组织	状态	操作
1	DC_1_HDMI1	root	在线	 
2	DC_1_HDMI2	root	在线	 
3	DC_1_VGA	root	在线	 

3. 若键盘配合解码卡电视墙或拼控器电视墙使用，在[拼控器电视墙列表]页签下选择电视墙（需要在软件客户端上创建好）。每个电视墙自动被分配一个电视墙编号（如1）。



电视墙编号	电视墙名称	操作
1	电视墙1	 

4. 完成上述操作后，即可在网络键盘上通过输入相机及解码通道的通道编号或电视墙编号进行视频上墙等操作。

3.4.5 云端编码设备

基础配置>设备管理>设备>云端编码设备

云端编码设备主要应用于广域网组网。先将支持宇视云的IPC/NVR注册至云账号，然后在平台上登录该云账号（需在线），即可管理该账号下的IPC、NVR设备。

说明:

在使用私有协议或国标协议将NVR添加到平台后，不建议再将其添加为平台的云端编码设备进行管。对于某些NVR款型，这种使用方式可能会导致个别服务的异常情况。

云账号	登录	刷新	在线					
我的云端设备		共享给我的云端设备						
+ 添加	删除	设备名称	请输入关键字					
云账号名称	设备名称	IP地址	所属服务器	所属组织	设备型号	设备连接模式	在线状态	操作
107	107	192.168.2.107	VMS	zhao	NVR	直连	在线	1 2 3 4
136	136	192.168.2.136	VMS	zhao	IPC	直连	在线	

功能操作	说明
登录云账号	输入账号信息，登录已经注册好的云账号。 登录成功后，云账号下的设备（若有）显示在列表中。 可登录多个云账号，管理多个云账号下的设备。登录多个云账号后，可点击左侧组织树上的云账号，查看对应账号下的设备。
管理云账号	管理平台上的云账号，包括刷新状态、退出登录、查看共享记录、取消共享。
添加云端编码设备	向指定在线云账号添加设备（不能添加平台设备）。添加时需输入设备名称和注册码。主从配置下可选择所属平台服务器。添加成功的设备显示在[我的云端设备]下；若登录成功，设备状态显示为“在线”。
编辑云端编码设备（1）	修改设备名；主从配置下可修改所属平台服务器。 若勾选[同步到云端]，修改后的设备名将被同步至云端；否则只修改平台上的设备名称。
删除云端编码设备（2）	将设备从当前云账号下删除。
共享云端编码设备（3）	将设备共享给一个或多个其他云账号。需要设置共享有效期并选择权限（设备侧已创建的用户）。
查看共享给我的云端编码设备	查看共享自其他云账号的设备。可以主动取消共享。
获取通道信息（4）	获取设备的通道信息，编辑通道名称。

3.4.6 门禁设备

基础配置>设备管理>门禁设备

添加宇视速通门、人脸门禁、ER-SR 1系列门禁控制器、ER-SR 2系列门禁控制器、人证终端。完成配置后，可在软件客户端上操作“门禁控制”模块。



说明:

第三方门禁设备在[基本配置>设备管理>门禁主机]下管理。

添加设备
✕

门禁类型:

* IP地址:

* 端口:

* 用户名:

密码:

* 设备名称:

* 所属组织:

描述:

① 一体机添加门禁设备后，会清除门禁设备人脸库数据，请提前做好数据备份

- 添加设备具体操作步骤请参见[普通编码设备](#)。



说明:

若ER-SR 1系列门禁控制器和平台不在同一网段可通过以下方法修改：

1. 将门禁控制器的网线连接至平台的网卡。
2. 单击<自动搜索>，找到该门禁控制器。
3. 单击对应门禁控制器操作列下的，弹出[修改IP地址]页面。
4. 修改门禁控制器IP地址和网关地址，使其与平台网段一致。
5. 单击<确定>后将门禁控制器重新连接至原组网即可在平台搜索到该设备。

- 添加时注意根据实际情况选择门禁类型并正确设置IP和端口号。
- 成功添加并上线的门禁主机处于“在线”状态，同时在[门禁通道]下自动添加门禁通道。



说明:

- 删除门禁设备会自动删除门禁通道。
- 添加人证终端后，可在[基本信息](#)中添加人员时选择采集设备进行人证信息采集，采集后的信息会填充到平台。

点击页面上方的<导出>可导出设备列表。

3.4.7 接入网关

基础配置>设备管理>接入网关

添加接入网关EZAgent，使平台接收和处理各品牌报警主机和门禁主机的报警，并允许用户通过软件客户端进行布/撤防、旁路/取消旁路、开/关门操作。更多信息，请见《EZAgent接入网关用户手册》和《综合监控一体化平台软件客户端用户手册》。

添加步骤

1. 单击<精确添加>。

添加设备✕

*设备名称:

*组织名称:

*IP/域名:

*端口:

*用户名:

密码:

*所属服务器:

备注:

 **说明:**

- “IP/域名”是EZAgent服务器所在PC的IP /域名。
- “用户名”是“admin”，密码是EZAgent服务器的密码。

- 成功添加并上线的接入网关处于“在线”状态，同时在平台Web客户端上显示接入网关上已经添加的报警主机和报警点通道、门禁主机及门禁通道。

 **说明:**

通过EZAgent接入的报警主机和门禁主机，不能在平台的Web客户端上添加他们的通道，只能在EZAgent上添加。

3.4.8 报警主机

基础配置>设备管理>报警主机

直接接入报警主机，使平台能够接收报警主机的报警，使用户可以在软件客户端上进行布/撤防、旁路/取消旁路等操作。

- 点击<添加>。
- 选择厂家和型号，完成所需设置。

添加报警主机
✕

*主机类型:

*组织名称:

*所属服务器:

*主机厂商:

*主机型号:

*主机名称:

用户名:

密码:

*IP 地址:

*端口:

*本地端口:

*扩展端口:

*本地扩展端口:

确定
取消



说明:

- “IP地址”是报警主机的IP或对应报警平台所在PC的IP。
- 如果需要在软件客户端上进行布/撤防、旁路/取消旁路，则需要设置用户名和密码。

3. 成功添加并上线的报警主机显示为“在线”状态。

单击页面上方的相关链接>[报警自定义](#)跳转至报警自定义页面，在该页面可自定义通用报警主机上报的报警类型。

3.4.9 门禁主机

基础配置>设备管理>门禁主机

直接接入门禁主机，使平台能够接收门禁主机的报警，使用户可以在软件客户端上进行开/关门等操作。

1. 点击<添加>。
2. 选择厂家和型号，完成所需设置。

添加门禁主机
✕

*主机类型:

*组织名称:

*所属服务器:

*主机厂商:

*主机型号:

*主机名称:

用户名:

密码:

*IP 地址:

*端口:

*本地端口:

*扩展端口:

*本地扩展端口:

确定
取消



说明:

- “IP地址”是门禁主机的IP或对应门禁平台(如纽贝尔门禁平台)所在PC的IP。
- 如果需要在软件客户端上进行开/关门操作，则需要设置用户名和密码。

3. 成功添加并上线的门禁主机显示为“在线”状态。

单击页面上方的相关链接>报警自定义跳转至报警自定义页面，在该页面可自定义通用门禁主机上报的报警类型。

3.4.10 安全网关

基础配置>设备管理>安全网关

添加安全网关，使平台接收和处理网络攻击报警。

1. 点击<精确添加>。

添加设备 ×

*设备名称:

*组织名称:

*IP/域名:

*端口:

*用户名:

密码:

*所属服务器:

备注:

2. 成功添加并上线的接入网关处于“在线”状态。

3.4.11 出入口设备

基础配置>设备管理>出入口设备

添加、管理停车场出入口设备。完成配置后，可在软件客户端上操作[停车场]模块。

添加设备
×

*设备名称:

*组织名称:

*IP/域名:

*端口:

*用户名:

密码:

确定
取消

点击<自动搜索>或<精确添加>添加设备（具体操作步骤请参见[普通编码设备](#)）。

3.4.12 通道

编码通道

基础配置>设备管理>通道>编码通道

- 查看编码设备的通道状态。
- 点击，访问通道所属设备的Web页面。
- 点击，编辑通道名称，选择通道的摄像机类型。



说明:

不同摄像机类型在资源树中显示的图标不同：枪机，球机，变焦变焦枪机。

- 点击(1)，导出设备通道信息到表格。在表格中修改通道名称后，点击(2)，导入表格，可批量修改通道名称。

通道名称	所属设备	所属设备序号	所属组织	状态	操作
192.168.17.21_V_02	192.168.17.21	2	root	■ 离线	
192.168.17.31_V_09	192.168.17.21	9	root	■ 离线	
192.168.17.21_V_12	192.168.17.21	12	root	■ 离线	
192.168.17.26_V_1	192.168.17.26	1	root	■ 在线	
192.168.17.31_V_1	192.168.17.31	1	root	■ 在线	

解码通道

基础配置>设备管理>通道>解码通道

- 查看解码设备的通道状态和能力。
- 点击，编辑通道名称。
- 点击(1)，导出设备通道信息到表格。在表格中修改通道名称后，点击(2)，导入表格，可批量修改通道名称。

通道名称	所属设备	所属设备序号	所属组织	分辨率 (默认)	分辨率 (最大)	状态	操作
DC_1_HDMI1	DC_1	1	root	SXGA60	64	■ 在线	
DC_1_HDMI2	DC_1	2	root	SXGA60	64	■ 在线	
DC_1_VGA	DC_1	3	root	SXGA60	36	■ 在线	



说明:

DC_1_VGA、DC_1_HDMI1和DC_1_HDMI2是内置解码器DC_1的解码通道。

报警通道

基础配置>设备管理>通道>报警通道

- 查看设备的报警输入通道和报警输出通道。勾选(1)查看指定类型的报警通道
- 在[操作]列中，点击(2)修改通道名称和报警类型（常开或常闭）。可启用或停用报警输入通道。对报警输出通道，可编辑“延续时间”，即报警类型改变后的持续时间。点击(3)，批量进行上述配置操作。
- 点击(4)，导出报警通道信息到表格。在表格中修改通道名称后，点击(5)，上传修改后的表格，可批量修改通道名称。

通道名称	所属设备	所属设备序号	所属组织	通道类型	状态	操作	类型
VMS-20A16-DT_I_1	VMS-20A16-DT	1	root	报警输入通道	■ 在线	(2)	常开
VMS-20A16-DT_I_2	VMS-20A16-DT	2	root	报警输入通道	■ 在线		常开
VMS-20A16-DT_I_3	VMS-20A16-DT	3	root	报警输入通道	■ 在线		常开
VMS-20A16-DT_I_4	VMS-20A16-DT	4	root	报警输入通道	■ 在线		常开
VMS-20A16-DT_I_5	VMS-20A16-DT	5	root	报警输入通道	■ 在线		常开

报警点通道

基础配置>设备管理>通道>报警点通道

添加报警点/报警主机通道至平台的报警主机。

添加
×

* 所属设备:

* 通道名称:

* 通道类型:

* 防区编号:

分区编号:

门禁通道

基础配置>设备管理>通道>门禁通道

成功添加我司的门禁设备后会添加对应的门禁通道。第三方门禁设备需手动添加门禁通道。

可根据需要设置通道名称、核验模式/开门模式、门编号、门方向、是否为考勤点（用于考勤打卡）等。（不同的门禁设备的配置项不同，请以实际界面为准）。

编辑
✕

*所属设备:

*通道名称:

*通道类型:

*核验模式:

*门方向:

考勤点:

确定
取消

3.4.13 关联资源

基础配置>设备管理>关联资源

将关联源（视频通道）与目标（报警输出通道）绑定。完成配置后，可以在软件客户端的[实况]页面手动触发报警输出。

1. 点击<分配>。
2. 在左侧勾选关联源，在右侧勾选关联目标。一个源可关联多个目标。点击<确定>。

关联资源
✕

说明：请先选择关联源。

关联源

源类型:

请输入关键字

- cloud
- NVR 192.168.2.100
- DC DC_1
- DC DC_2
- DC DC_3
- NVR 192.168.2.99
- NVR 192.168.2.107
 - 192.168.2.107_V_1
 - 192.168.2.107_V_3
 - 192.168.2.107_V_4
- NVR 192.168.2.109
- 192.168.1.30
- DX 192.168.2.124
- 192.168.2.50

关联目标

目标类型:

请输入关键字

- 根组织
- cloud
- NVR 192.168.2.100
- DC DC_1
- DC DC_2
- DC DC_3
- NVR 192.168.2.99
- NVR 192.168.2.107
- NVR 192.168.2.109
- 192.168.1.30
- DX 192.168.2.124
- 192.168.2.50
- 192.168.2.252
- VMS-B200-A16@R

确定
取消

- 在软件客户端上播放该摄像机的实况时，点击浮动工具栏中的  按钮，在弹出的对话框中手动触发关联目标的外接报警设备（如报警灯）。



3.5 服务器管理

查看中心服务器（包括主机和备机）和分布式服务器（指从机）信息和状态；指定从机的工作模式和备份模式；分配主从服务器下的设备资源。

3.5.1 中心服务器

基础配置>服务器管理>中心服务器

查看中心服务器的信息和状态。点击  查看接入能力和带宽能力。



3.5.2 分布式服务器

基础配置>服务器管理>分布式服务器

查看从机信息和状态，删除主机下的从机；配置归属服务器或备用服务器。

名称	IP	序列号	类型	工作模式	工作状态	状态	操作
VMS_SLAVE001	206.9.10.30	从机	归属服务器	故障	■ 离线 - 从机未注册	

- 点击  查看从机的接入能力和带宽能力。

- 点击  删除从机。
- 点击  设置从机的工作模式：归属服务器或备用服务器。

编辑

* 服务器名称:

工作模式: 归属服务器 备用服务器

归属服务器正常工作时，备用服务器处于空闲状态。若归属服务器发生故障或者下线（工作状态由“正常”变为“故障”），空闲的备用服务器将接管业务（“工作状态”由“空闲”变为“正在接管”），直到归属服务器恢复正常。恢复正常的归属服务器将重新接管业务并与备用服务器同步数据。

说明:

- 只有admin有权修改工作模式。修改工作模式会清空服务器数据并重启服务器。当服务器下存在设备时不能修改工作模式。
- 一台备用服务器同一时刻只能接管一台归属服务器。
- 备用服务器不能自动回传录像给归属服务器。
- 备用服务器不支持缓存补录、录像备份、录像锁定和标签功能。

3.5.3 资源重配

基础配置>服务器管理>资源重配

分配主从机下的设备资源（包括云端设备），达到负载均衡等目的。

分配到
自动分配
还原
保存
资源详情
ⓘ 可拖拽（非国标和UNP接入）设备、组织至任意服务器；建议尽量平衡。

请输入关键字 🔍

VMS
📄

 192.168.1.182

 192.168.4.212

 192.168.4.200

 192.168.5.208

 192.168.4.114

 192.168.4.141

 192.168.5.203

 192.168.4.104

 192.168.4.252

 192.168.4.168

 192.168.4.108

VMS @从机
📄

 192.168.5.208

 192.168.4.108

 192.168.4.100

 192.168.4.208

 192.168.4.208

 192.168.4.178

 192.168.4.208

 192.168.4.125

 192.168.4.104

 192.168.5.204

 192.168.4.223

- 直接拖拽至目标主机或从机下。
- 点击<自动分配>，自动分配所有设备。
- 点击<还原>，恢复页面加载时的初始状态。
- 点击<资源详情>可查看该页面设备及通道的汇总信息。
- 点击主机或从机名称旁的  查看主机/从机下的设备编码通道详情，其中不含智能编码设备。

24

说明:

- 在从机的设备列表上，点击某台设备的删除按钮（光标靠近设备时出现，如  192.168.4.232  ），该设备将从当前从机下移除并划归给主机。
- 备用服务器只有当工作状态为“正在接管”时才显示。
- 所有操作需单击<保存>才可生效。
- 重新分配资源会影响设备录像计划，请谨慎操作。
- 若需在从机上添加国标设备，需要在设备侧将服务器IP设定为从机IP。
- 若需在从机上添加UNP设备，需要在设备侧将UNP服务器地址设定为从机IP。

3.6 批量配置

3.6.1 批量修改密码

基础配置>批量配置>批量修改密码

批量修改主机或从机下直连编码设备（目前仅NVR和IPC）的密码。

不支持修改国标接入的设备和云端设备。只能在主机上批量修改从机下的设备密码。

1. 在左侧选择组织，在右侧勾选设备，点击<批量修改密码>。

<input type="checkbox"/>	设备名称	设备类型	所属组织	接入协议	在线状态	操作	提示
<input type="checkbox"/>	192.168.5.171	IPC	根组织	私有	<input checked="" type="checkbox"/> 在线		
<input type="checkbox"/>	192.168.5.91	IPC	根组织	私有	<input checked="" type="checkbox"/> 在线		

2. 两次输入新密码后点击<确定>。

3.6.2 批量码流加扰

基础配置>批量配置>批量码流加扰

对设备进行码流加扰设置，将网络传输的视频流加扰，提高安全性。

1. 在左侧组织列表中选择组织。
2. 勾选视频通道。可点击顶部的批量选择框，勾选当页显示的所有通道。
3. 点击<开启>。单个通道可以点击操作栏下的  按钮配置码流加扰。

<input checked="" type="checkbox"/> 开启	<input type="checkbox"/> 关闭	刷新	请输入关键字				
<input type="checkbox"/>	通道名称	所属设备	所属组织	接入协议	在线状态	状态	操作
<input type="checkbox"/>	192.168.5.101_V_1	192.168.5.101	根组织	私有	<input checked="" type="checkbox"/> 在线	关闭	
<input type="checkbox"/>	192.168.5.102_V_1	192.168.5.102	根组织	私有	<input checked="" type="checkbox"/> 在线	关闭	
<input type="checkbox"/>	192.168.5.117_V_1	192.168.5.117	根组织	私有	<input checked="" type="checkbox"/> 在线	关闭	

说明:

该功能仅支持私有协议接入的设备。

3.6.3 NVR批量操作

基础配置>批量配置>NVR批量操作

对在线NVR进行关机、重启操作。

说明:

- 该功能需要NVR版本配套。当NVR不支持该操作时，系统会有提示。
- 该功能不支持国标接入的设备。

🔌 NVR批量关机		⚙️ NVR批量重启		🔄 刷新			
<input type="checkbox"/>	设备名称	设备类型	所属组织	接入协议	在线状态	操作	
<input type="checkbox"/>	192.168.171.04	NVR	root	私有	■ 在线	<input type="checkbox"/>	⏻ ⚙️
<input type="checkbox"/>	20121111	NVR	root	私有	■ 在线	<input type="checkbox"/>	⏻ ⚙️

关机

- 关机操作。
 - 批量关机：在列表中勾选NVR，单击<NVR批量关机>。
 - 单个关机：单击NVR对应的⏻。
- 单击<刷新>，关机的NVR从界面上消失。

重启

- 重启操作。
 - 批量重启：在列表中勾选NVR，单击<NVR批量重启>。
 - 单个重启：单击NVR对应的⚙️。
- 在弹出的[提示]窗口，单击<确定>。重启过程中NVR状态显示“离线”。
- 一段时间后单击<刷新>，重启完成的NVR状态显示“在线”。

3.6.4 批量编码参数配置

基础配置>批量配置>批量编码参数配置

对私有协议接入的IPC/NVR或ONVIF协议接入的IPC进行批量编码参数配置。支持对多台相同型号的IPC或一台NVR进行配置。以NVR为例。

- 勾选一台NVR，点击<批量配置>。

⚙️ 批量配置		🔄 刷新		请输入关键字			
<input type="checkbox"/>	设备名称	IP地址	设备型号	版本	序列号	在线状态	操作
<input type="checkbox"/>	192.168.5.171	192.168.5.171	PARK_2	1		■ 在线	⚙️
<input type="checkbox"/>	192.168.5.91	192.168.5.91	QIPC-B	04		■ 在线	⚙️

- 勾选通道，进行配置。界面只显示支持的码流类型；不支持的码流类型会被过滤掉。

参数配置(192.168.5.91) ✕

主流	辅流	第三流
编码格式: <input type="text" value="H.264"/>	编码格式: <input type="text" value="H.264"/>	编码格式: <input type="text" value="H.264"/>
分辨率: <input type="text" value="1920×1080(1080P)"/>	分辨率: <input type="text" value="720×576(D1)"/>	分辨率: <input type="text" value="352×288(CIF)"/>
帧率: <input type="text" value="25"/>	帧率: <input type="text" value="25"/>	帧率: <input type="text" value="25"/>
码率: <input type="text" value="4096"/> 128-16384	码率: <input type="text" value="1024"/> 128-16384	码率: <input type="text" value="128"/> 128-16384
图像质量: 质量优先 <input type="range" value="50"/> 码率优先	图像质量: 质量优先 <input type="range" value="50"/> 码率优先	图像质量: 质量优先 <input type="range" value="50"/> 码率优先
I帧间隔: <input type="text" value="50"/> 10-250	I帧间隔: <input type="text" value="50"/> 10-250	I帧间隔: <input type="text" value="50"/> 10-250
U-Code: <input type="text" value="关闭"/>	U-Code: <input type="text" value="关闭"/>	U-Code: <input type="text" value="关闭"/>

- 点击<确定>保存配置。

3.6.5 设备升级

基础配置>批量配置>设备升级

对设备进行升级操作。

1. 在左侧组织列表中选择所需组织。
2. 勾选需要升级的设备，单击<检查更新>。有新版本会在可升级版本中显示。
3. 若有可升级版本，单击<升级>升级所选设备。



升级过程中可单击<刷新>获取最新的升级状态。

3.7 录像计划

通过时间模板自定义不同摄像机在指定时间段的录像动作。

3.7.1 时间模板

基础配置>录像计划>时间模板

时间模板用于录像计划，包括具体时间及对应的录像策略。系统自带一个全天录像的时间模板（All-day）。用户可自行创建时间模板，用于录像计划。

 说明:

- 可修改All-day模板名称，但不能删除模板。
- 时间模板中的假日需要在[系统配置>基本配置>假日配置]中配置并开启才生效（见假日配置）。

1. 点击<添加>，然后按照图示步骤新建时间模板。

添加时间模板
✕

模板名称: 1

复制模板 2

✎ 编辑 5 ↺ 重置 6

每天最多可设置8个时段

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
星期日																									
星期一																									
星期二																									
星期三																									
星期四																									
星期五																									
星期六																									
假日																									

4

✎ 擦除

- 定时计划
- 运动检测
- 事件
- 报警计划
- 动测和报警
- 动测或报警

3

假日说明: 配置假日前请先启用假日日期, 否则配置不生效。

备注: ✎

确定

取消

编号	说明
1	模板名称必须唯一。
2	勾选后, 选择一个已有模板, 在该模板基础上修改编辑 (不会改变原有模板)。
3	点击某个类型, 在左侧点击或拖动鼠标进行绘制, 使当前类型将在对应时间段内生效。
4	点击后, 在左侧点击或拖动鼠标, 删除生效的时间段。
5	点击进行精确设置。可使用“复制到”功能, 将某天的设置复制给其他天 (先勾选, 再点击<复制>)。
6	点击清除所有设置。

2. 参照以下说明设置录像类型。

类型	说明
定时计划	根据时间模板时间段定时录像。
运动检测	运动检测报警发生时录像。
事件	除以下报警类型外, 其余报警发生时录像。 运动检测、遮挡检测、开关量 (报警输入)、高温报警、低温报警、风扇故障、电箱高温、电箱烟雾、智能跟踪、虚焦检测、人形检测、入梯检测、人员密度普通/中度/严重报警。
报警计划	以下报警类型发生时录像。

类型	说明
	包括遮挡检测、开关量（报警输入）、高温报警、低温报警、风扇故障、电箱高温、电箱烟雾、智能跟踪、虚焦检测、人形检测、入梯检测、人员密度普通/中度/严重报警。
动测和报警	运动检测和报警计划的报警同时发生时录像（比如：运动检测和遮挡检测同时发生时）。
动测或报警	运动检测或报警计划的报警任意一个发生时录像（比如：运动检测和遮挡检测任意一个发生时）。

成功创建的时间模板出现在列表中，可根据需要进行编辑或删除。

3.7.2 录像计划

基础配置>录像计划>录像计划

配置录像计划，使平台根据时间、录像类型、码流类型等设置对选定相机进行录像。

1. 点击<添加>，然后参照步骤新建录像计划。

2. 选择摄像机。
3. 选择时间模板（或点击+新建）。
4. 选择录像使用的码流类型。
5. 选择所属盘组（普通存储或IPSAN）。
6. 录像计划默认处于启用状态。清空复选框将停止录像计划。
7. 在备注栏中输入对该录像计划的补充描述。
8. 新建的录像计划出现在列表中。

说明:

- 必须为联动录像的摄像机配置并启用录像计划；否则联动录像不生效。详细信息请见[报警配置](#)。
- 平台支持缓存补录功能。对于配置有录像计划且支持缓存补录功能的IPC（包括NVR下的IPC），网络连接中断时，录像保存至IPC的SD卡或NVR上；网络恢复后，SD卡或NVR上的录像将自动补录到平台上。
- 对于第三方IPC，若所选码流类型为不支持的视频格式（如MJPEG），录像将失败，[录像计划]页面的“诊断结果”列中将显示“码流格式不支持”。

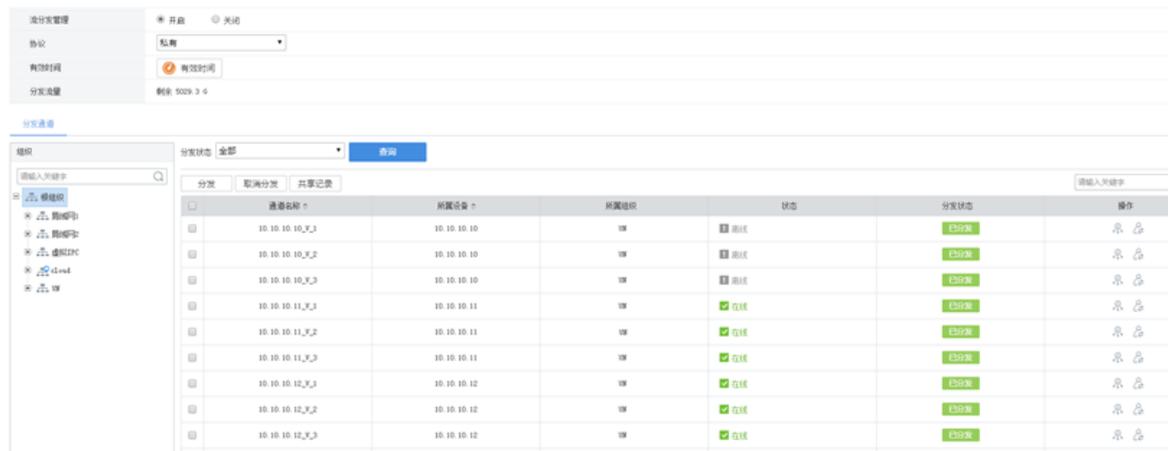
其他操作

- 编辑录像计划：单击录像计划操作列下的  或勾选需要修改的录像计划，单击页面上方的<编辑>，在弹出的[编辑录像计划]中修改录像计划，单击<确定>完成修改。
- 开启录像计划：单击录像计划操作列下的  或勾选需要开启的录像计划，单击页面上方的<开启>，开启后录像计划才生效。
- 关闭录像计划：单击录像计划操作列下的  或勾选需要关闭的录像计划，单击页面上方的<关闭>，关闭后录像计划不生效。
- 删除录像计划：单击录像计划操作列下的  或勾选需要删除的录像计划，单击页面上方的<删除>删除录像计划。
- 快速跳转：单击页面上方的[相关链接]，可在下拉列表中选择<录像状态>或<容量配置>快速跳转至相关页面。

3.8 流分发管理

基础配置>流分发管理

选择宇视或其他CDN服务提供商分发平台通道的视频流。



说明:

最多可分发40路1080P或100路D1相机，流分发路数可能会因为码率和编码格式的不同而变化，具体请以实际为准。

- 流分发管理：开启时可对云分发进行管理。关闭将停止所有通道的流分发。
- 有效时间：只有在有效时间内进行流分发。
- 协议：选择“私有”（宇视云）或“RTMP”（第三方云服务）。

3.8.1 私有协议

- 分发流量：流分发业务的当前剩余可用流量。剩余流量为0时自动停止分发。
- 在线状态：通道在平台上的在、离线状态。通道被删除或下线时，平台停止该通道的推流。

- 分发：勾选通道后点击<分发>，查看分发状态。“已分发”表示该通道支持分发，“未分发”表示该通道不支持分发。对于分发状态为“已分发”的通道，当用户在客户端（如手机APP）上播放该通道的实况时，平台会推送该通道的视频流。
- 点击[操作]列中的共享图标，允许共享对象在指定时间段查看共享并支持分发的通道的视频。

3.8.2 RTMP

RTMP的最大推流数为128。

- 点击 [分发](#) >> 添加分发通道。可选择特定码流类型进行添加。
- 设置分发的码流类型和URL。URL需遵循特定的格式要求。
- 状态：通道在平台上的在、离线状态。通道被删除或下线时，平台停止该通道的推流。
- 分发：勾选通道后点击<批量分发>。查看分发状态。状态为“已分发”表示平台正在推送该通道的视频流。
- 要取消分发，勾选通道后点击<删除>。

4 报警配置

报警配置是对报警时间模板、报警级别、订阅用户进行配置，当报警触发时，可按照预先配置执行联动动作。

通过报警配置功能可对报警进行配置和订阅，提前配置好报警，当发生告警时，可以联动触发录像、发送邮件、抓图等动作，一方面便于用户查看告警的具体情况，另一方面实现系统自动对告警做应急处理。并且可对报警级别进行自定义，方便后期通过等级区分不同严重程度的报警。例如，管理员设置夜间发生火点报警时，启用蜂鸣器报警，人员可在听到报警后及时疏散。

支持对报警、时间模板、报警订阅进行配置，自定义报警级别、设置通讯录用于联动邮件知会指定人员。

4.1 报警配置

报警配置>报警配置

1. 点击<添加>，参照图示步骤新增报警配置。

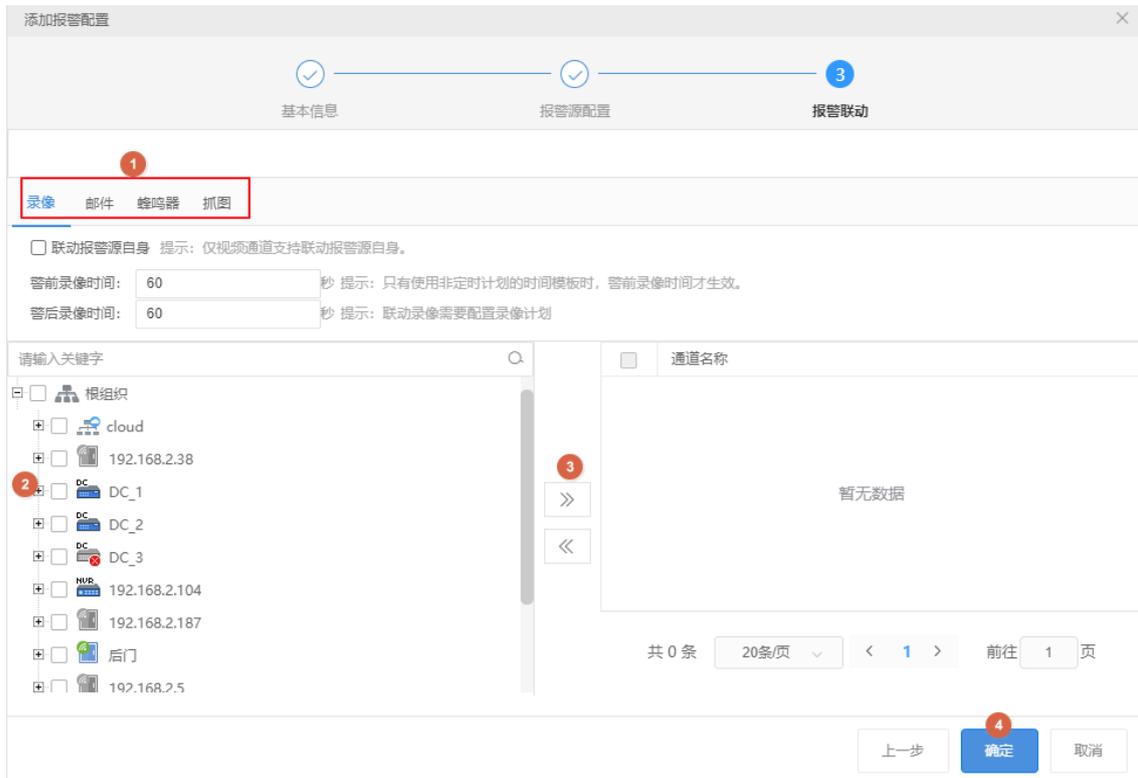
编号	说明
1	报警配置名称必须唯一。
2	选择时间模板。可点击+新建。 报警配置在所选时间模板设定的时间范围内生效。
3	勾选时，该报警配置才生效。
4	开启后，报警信息将被上传到宇视云。 说明： 关闭“推送到宇视云”将同时关闭“图片推送到宇视云”。

2. 完成报警配置名称、时间模板等设置。



编号	说明
1	选择报警源类型。 说明： 实际显示的类型与平台型号、版本有关，上图仅为示例。请以实际界面为准。
2	选择报警源。
3	选择报警类型。

3. 设置报警源和报警类型。当报警源发生指定类型的报警时，将触发联动对象执行指定动作。最多可添加2000条报警源和报警类型组合。
4. 设置联动动作和联动对象。当指定报警源发生指定类型的报警时，联动对象将执行指定动作。



编号	说明
1	选择联动动作。
2	选择联动对象。
3	配置联动动作（见下表）。

表 4-1: 配置报警联动动作

联动动作	说明
录像	<ul style="list-style-type: none"> 联动报警源自身：勾选后发生报警将联动报警源自身去录像，取消勾选可在下方选择需要联动的相机并单击将通道添加至右侧，支持同时联动多个通道进行录像。 警前录像时间：完成配置后，报警录像的开始时间将包含设定的时间。比如，设定警前录像时间为10秒，报警发生时间为12:00:00，那么报警录像的开始时间为12:00之前10秒钟，即11:59:50。 警后录像时间：对于可自动恢复的持续性报警，如运动检测、视频丢失等，警后录像时间x表示录像将在报警恢复x秒后停止；对于无法自动恢复的非持续性报警，如IP冲突、非法访问等，警后录像时间x表示录像将在报警发生x秒后停止。 <p>说明： 配置联动录像必须为联动对象配置并开启录像计划。</p>
邮件	需完成邮件相关设置。
蜂鸣器	需勾选[启用蜂鸣器]。
抓图	<ul style="list-style-type: none"> 联动报警源自身：勾选后发生报警将联动报警源自身去抓图，取消勾选可在下方选择一个需要联动的相机进行抓图。 抓图时间间隔：将每隔一个时间间隔抓图一次，直到达到最大抓图次数为止。

联动动作	说明
	<ul style="list-style-type: none"> 最大抓图次数：设置最大抓图次数，报警发生后，将在抓图达到设置次数后停止。 图片推送到宇视云：在基本信息中开启“推送到宇视云”后在此处勾选[图片推送到宇视云]，联动抓图将被上传到云端，可通过移动客户端查看。该功能需设备侧开启宇视云并支持云存储。若在基本信息中关闭“推送到宇视云”，则勾选“图片推送到宇视云”也不生效。 <p> 说明:</p> <ul style="list-style-type: none"> 仅自定义报警和如下报警类型支持配置报警联动抓图：运动检测、视频丢失、报警输入、遮挡检测、音频检测、IPC离线、越界检测、区域入侵、人脸检测、场景变更、虚焦检测、人脸识别匹配报警、人脸识别不匹配报警、人员聚集、智能跟踪、徘徊检测、车辆识别匹配报警、车辆不识别匹配报警、物品搬移、火点报警、人形检测、防区报警、挟持报警、防区旁路操作、防拆报警、防拆报警恢复。 配置联动抓图需要为联动对象分配图片容量（见容量配置）。告警抓图不支持对车牌/车辆图片的单独抓拍和上传。

成功创建的报警配置出现在列表中。可以删除、开启、关闭报警配置。关闭的报警配置不生效。

4.2 时间模板

报警配置>时间模板

为报警配置设定时间模板。详细信息可参考[时间模板](#)。

4.3 邮件记录

报警配置>邮件记录

如果在**报警配置**中配置了联动邮件，需先在添加邮件地址作为联动邮件的收件人。在添加时可点击<发送测试邮件>测试邮件地址是否可用。

 **说明:**
发送测试邮件前需完成邮件服务器配置（见[邮件](#)）。

4.4 报警级别自定义

报警配置>报警级别自定义

根据报警类型划分级别，以便区分不同报警的严重程度。共5个级别（1-5级），1级最严重，用红色表示。

在左侧树上选择报警源类型（如设备），在右侧对应的[报警级别]下拉框中选择报警级别。配置直接保存。

自定义报警级别 2		请输入关键字
报警类型	报警级别	
<input type="checkbox"/> 硬盘离线	■ 1级	
<input type="checkbox"/> 硬盘异常	■ 1级	
<input checked="" type="checkbox"/> 录像存储空间即将满 1	■ 1级	
<input type="checkbox"/> 录像存储空间满	■ 1级	
<input type="checkbox"/> 设备上线	■ 5级	
<input type="checkbox"/> 设备离线	■ 1级	

若要批量配置：勾选报警类型（1），点击<自定义报警级别>（2）。在出现的对话框中选择报警级别，然后点击<确定>。

4.5 报警订阅

对指定设备的指定报警类型进行订阅，实现仅在客户端接收需要关注的告警。

类型	描述	区别
客户端报警订阅	对客户端的用户订阅需要关注的实时报警。	<ul style="list-style-type: none"> 仅过滤实时报警；仍可查看全部历史报警记录。 需指定报警接收用户。 报警订阅开启后全时段生效。
设备报警订阅	对设备报警进行过滤，仅接收需要关注的设备报警。	<ul style="list-style-type: none"> 订阅规则针对于实时报警和历史报警。 订阅规则对全部用户生效。 可对报警订阅设置有效时段。

2种报警订阅类型可以只配置其一，也可以同时配置。

同时配置时，[设备报警订阅]规则的优先级高，即：

- 当[设备报警订阅]接收A报警时，[客户端报警订阅]订阅A报警后指定用户才能接收A报警，[客户端报警订阅]未订阅A报警则指定用户不能接收A报警。
- 当[设备报警订阅]过滤了B报警；[客户端报警订阅]即使订阅B报警也无法推送给指定用户。

4.5.1 客户端报警订阅

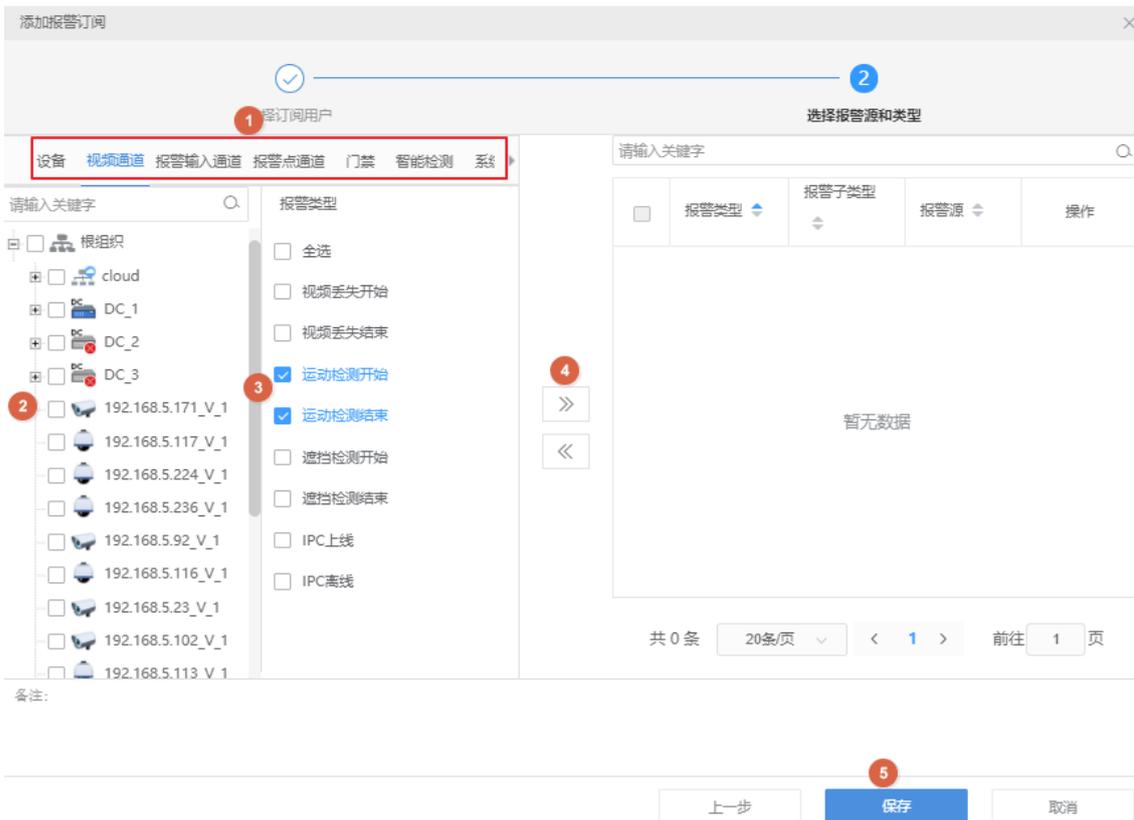
报警配置>客户端>客户端报警订阅

添加报警订阅，使指定用户只接收指定报警源上报的指定类型的实时报警消息；其他报警消息将被过滤掉（仍可查询已过滤告警的历史记录）。

1. 点击<添加>，进入[添加报警订阅]界面。
2. 选择报警订阅用户。

编号	说明
1	报警订阅名称必须唯一。
2	勾选“启用”后，报警订阅才生效。
3	勾选订阅用户。

3. 选择报警源和报警类型。



编号	说明
1	选择报警源类型。  说明： 实际显示的类型与平台型号、版本有关，上图仅为示例。请以实际界面为准。
2	选择报警源，只接收指定报警源的报警。
3	选择报警类型，只接收选定类型的报警。

4. 成功创建的报警订阅出现在列表中。可以删除、开启、关闭报警订阅。关闭的报警订阅不生效。

说明：

- 报警订阅默认开启。如果关闭，即使配置了报警订阅，客户端也接收不到任何报警消息。
- 非报警订阅用户默认接收全部报警消息。如需为某一用户屏蔽所有报警消息，只需将该用户添加为报警订阅用户，但不指定任何报警源，在[选择报警源和类型]步骤中直接点击<保存>即可。
- 历史报警能查询到所有报警信息，包括订阅报警与非订阅报警。

4.5.2 设备报警订阅

报警订阅>设备>设备报警订阅

通过配置设备报警订阅规则，可以仅接收需要关注的设备告警，过滤掉不关注的设备告警（过滤掉的告警不会保存历史告警记录）。对设备订阅告警时可设置有效时间段。

- 规则A：添加需要接收的报警信息并订阅，未添加默认过滤。

- 规则B：添加需要过滤的报警信息并订阅，未添加默认接收。

规则动态提示：启用“过滤下线告警”(规则B)

规则A——添加需要接收的报警信息并订阅，未添加默认过滤

规则B——添加需要过滤的报警信息并订阅，未添加默认接收

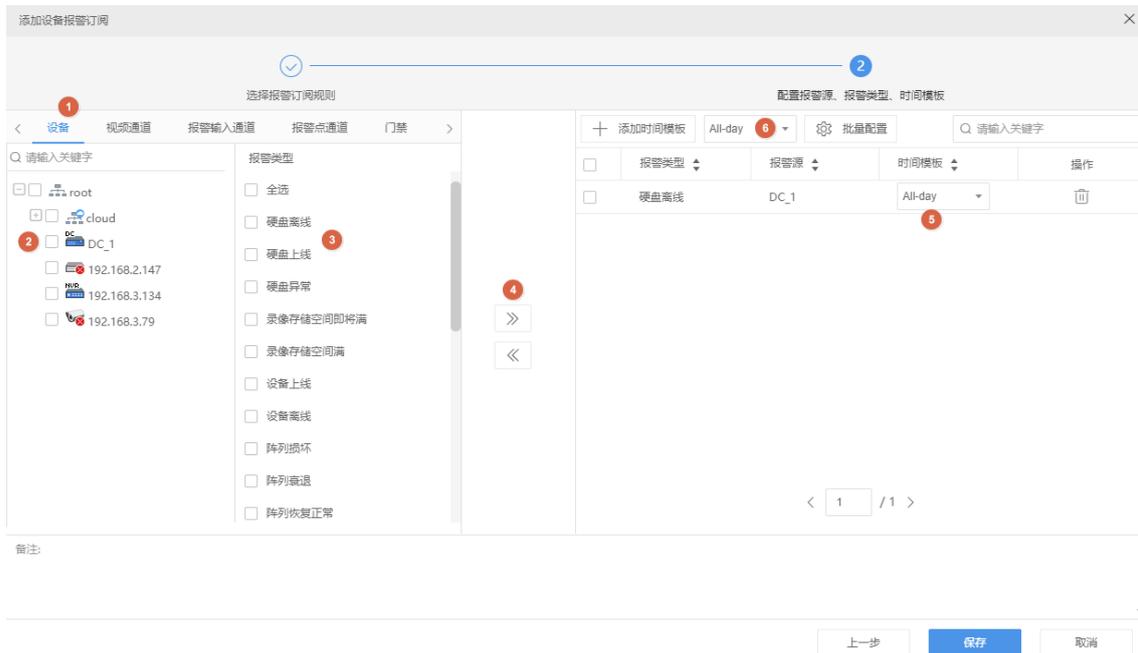
+ 添加		删除		Q 请输入关键字	
<input type="checkbox"/>	设备报警订阅预案名称	备注	订阅规则	状态	操作
<input type="checkbox"/>	订阅告警		规则A	■ 关闭	🔍 🗑️ ⌂
<input type="checkbox"/>	订阅硬盘告警		规则A	■ 关闭	🔍 🗑️ ⌂
<input type="checkbox"/>	过滤下线告警		规则B	■ 开启	🔍 🗑️ ⌂

添加报警订阅预案

1. 点击<添加>，进入[添加设备报警订阅]界面。

编号	说明
1	名称必须唯一。
2	如果勾选“启用”，则添加预案后即启用订阅；您也可以不勾选“启用”，添加预案完成后再按需启用。
3	选择规则A或规则B。

2. 单击<下一步>，配置报警源、报警类型、时间模板。



编号	说明
1	选择报警源类型。  说明: 实际显示的类型与平台型号、版本有关，上图仅为示例。请以实际界面为准。
2	选择报警源设备，只接收指定设备的报警。
3	选择报警类型，只接收指定类型的报警。  说明: 不同报警源支持的报警类型不同。
4	点击《》，将所选报警源和报警类型加入右侧列表。
5	选择时间模板，仅在时间模板允许的时段内订阅报警。  说明: <ul style="list-style-type: none"> 自定义添加时间模板：点击<添加时间模板>，操作参见时间模板。 批量配置：在⑥处选择一个时间模板，点击<批量配置>，可对所有报警类型应用时间模板。

3. 单击<保存>。

管理报警订阅预案

- 开启/关闭：单击操作栏的  开启 /  关闭报警订阅预案。



说明:

- 只有开启的预案才会生效。
- 同时只能开启一个报警订阅预案。如果已有预案启用中，启用新预案会关闭原有预案。
- 修改：单击操作栏的  ，可修改报警订阅预案的配置。
- 删除：单击操作栏的  ，或勾选预案，单击<删除>，可删除对应项。

时间模板

报警订阅>设备>时间模板



说明: 此界面创建的时间模板专用于“设备报警订阅”，不会影响其他需要时间模板的功能。

支持预先创建好时间模板，配置报警订阅生效时间，从而可在报警订阅时快速应用时间模板。

1. 单击<添加>，进入[添加时间模板]界面。

添加时间模板
✕

*模板名称:

复制模板

All-day

每天最多可设置8个时段

0 2 4 6 8 10 12 14 16 18 20 22 24

星期日

星期一

星期二

星期三

星期四

星期五

星期六

假日

报警订阅

假日说明：配置假日前请先启用假日日期，否则配置不生效。

备注:

编号	说明
1	模板名称不可重复。
2	勾选[复制模板]，从下拉框中选择一个模板，在该模板基础上进行编辑。原有模板不会改变。
3	点击<编辑>，精确设置每日时段。 完成某一天的设置后，可使用复制功能，将设置复制给其他时间。 📌 说明：假日需要在[系统配置>基本配置>假日配置]中配置并开启才生效（见假日配置）。
4	点击<擦除>，可使用光标在时间网格上拖动，擦除不需要的时间段。

2. 单击<确定>保存

4.6 报警自定义

4.6.1 报警自定义

报警配置>报警自定义>报警自定义

自定义字视报警主机或门禁主机上报的报警。

1. 单击<添加>。
2. 根据以下说明自定义报警。

添加
✕

*报警源类型:

*第三方报警类型:

*报警类型:

确定

取消

功能	描述
报警源类型	对接报警源的类型，支持报警主机或门禁主机。
第三方报警类型	报警源侧的报警类型。
报警类型	自定义输入报警展示在平台的类型，后续该报警上报时将展示为此类型。

- 单击<确定>完成添加，自定义报警的报警级别默认为1级，可在[报警级别自定义](#)中自行修改。

4.6.2 通用报警

报警配置>报警自定义>通用报警

支持在平台上添加设备侧 (AIBox/EIA) 的报警类型，从而可以接收设备上报的告警。

↓ 导入通用报警 🗑️ 删除 ↑ 导出
Q 请输入关键字

□	序号	报警类型	报警类型描述	状态	操作
□	1	ChannelBlockageDetection	逃生通道堵塞	■ 关闭	⊖
□	2	FireDetection	明火检测	■ 开启	⊖
□	3	FumesAlarmBegin	烟雾检测	■ 开启	⊖
□	4	AbnormalParkingDetection	异常停车事件	■ 开启	⊖

导入通用报警

- 单击<导入通用报警>，在[导入]界面，单击<下载导入模板>获取模板。

导入
✕

模板中带星号(*)字段为必填项。

文件保存路径
📁

下载导入模板

确定

取消

- 在模板中填写报警类型相关信息 (最多256个)。

序号 (*)	报警类型 (长度限制为1-64位)	报警类型描述 (长度限制为1-64位)	状态 (0-关闭, 1-开启)

- 报警类型：和设备侧的报警类型字段一致。
- 报警类型描述：在平台上展示的报警名称，可自定义。
- 状态：0-关闭，1-开启；开启后，平台才可接收该类型的报警。

- 在[导入]界面，单击📁，选择填写好的模板。单击<确定>导入。

开启/关闭通用报警

开启后，平台才可接收该类型的报警。

在列表中，单击报警类型对应的  开启；单击  关闭。

修改报警类型描述

在输入框中编辑描述，鼠标点击空白区域即可保存。

删除通用报警

在列表中勾选通用报警，单击<删除>。

导出通用报警

单击<导出>，以.csv文件导出通用报警。

5 录像备份

通过录像备份功能，可创建备份任务，筛选需要备份的录像类型，自动或手动将相机上的录像备份到平台或本地，保护录像不被意外损坏或丢失。

5.1 自动备份

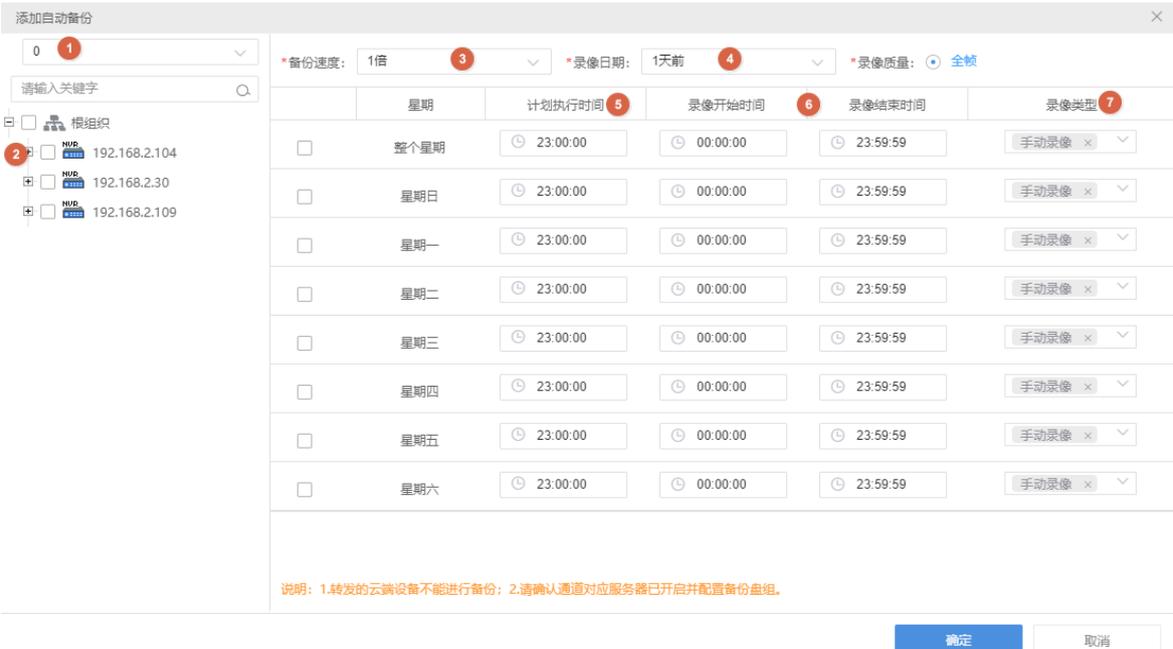
录像备份>自动备份

创建备份任务，自动按计划将IPC或NVR上的录像备份到平台上存储。

说明:

- 配置备份计划前需要先在平台上配置用于备份的存储空间（请见[容量配置](#)和[盘组属性](#)）。
- 连接模式是“转发”的云端编码设备不支持自动备份功能（在[[基础配置](#)>设备管理>云端编码设备]页面下查看）。

单击<添加>，参照图示步骤新建备份任务。



添加自动备份

0 

请输入关键字 

 根组织

*备份速度: 1倍  *录像日期: 1天前  *录像质量:  全帧

	星期	计划执行时间 	录像开始时间 	录像结束时间	录像类型 
<input type="checkbox"/>	整个星期	 23:00:00	 00:00:00	 23:59:59	手动录像  
<input type="checkbox"/>	星期日	 23:00:00	 00:00:00	 23:59:59	手动录像  
<input type="checkbox"/>	星期一	 23:00:00	 00:00:00	 23:59:59	手动录像  
<input type="checkbox"/>	星期二	 23:00:00	 00:00:00	 23:59:59	手动录像  
<input type="checkbox"/>	星期三	 23:00:00	 00:00:00	 23:59:59	手动录像  
<input type="checkbox"/>	星期四	 23:00:00	 00:00:00	 23:59:59	手动录像  
<input type="checkbox"/>	星期五	 23:00:00	 00:00:00	 23:59:59	手动录像  
<input type="checkbox"/>	星期六	 23:00:00	 00:00:00	 23:59:59	手动录像  

说明: 1.转发的云端设备不能进行备份; 2.请确认通道对应服务器已开启并配置备份盘组。

编号	说明
1	选择服务器。如果配置了从机，可以选择主机或从机。若配置从机备份，需要在从机上进行从机盘组的配置。

编号	说明
2	选择要备份的通道。
3	备份速度越高越占用平台的存储能力。
4	备份多少天前的录像。比如选择“1天前”，那么星期一执行的任务将备份星期天的录像。 不能备份当天的录像
5	指备份计划的执行时间。当计划执行时间等于平台的系统时间时，生成相应的备份任务并按照配置开始进行备份。每个计划中的任务依次执行；到时间未执行的任务处于等待状态。
6	录像开始时间和录像结束时间：指要备份的录像段的起止时间。
7	选择要备份的录像类型，如手动录像、运动检测等。

总存储能力：256（单位：路）

占用的存储能力=录像计划占用的存储能力+备份计划占用的存储能力

录像计划占用的存储能力=录像计划数
举例：2个录像计划占用2路存储能力

 说明：
一个录像计划，无论是否开启，无论时间模板的时间段是否为完整的一天，均占用一路。

备份计划占用的存储能力=备份计划数*备份速度*录像类型占用的存储能力

 说明：

- 备份速度：1/2/4/8倍数分别占用1/2/4/8路存储能力
- 录像类型：包括普通（即定时）或事件（包括手动录像、运动检测、报警输入、视频丢失、音频异常）
- 每个普通类型占用1路存储能力；n个普通类型占用n路
- 每个事件类型占用0.2路存储能力；n个事件类型占用n*0.2路
- 每个普通类型+事件类型占用1路存储能力
- 国标设备，每个备份计划的录像类型都按1路存储能力计算，无论录像类型个数。

 说明：

如果系统提示创建的备份任务超出了存储能力，可在[运维统计>服务器统计>存储能力]页面查看平台的存储使用情况（见[存储能力](#)）。

成功创建的备份计划出现在列表中。可以暂停、修改、删除任务，查看任务详情。

 说明：

- 在备份任务开始后修改设置（如录像结束时间）不会改变当前任务；修改的设置在下一次任务生成时生效。
- 如果自动备份由于某种原因被中断（比如NVR离线），可在条件恢复后，点击<批量恢复>，恢复全部备份任务。

5.2 本地备份

录像备份>本地备份

将录像手动备份到U盘上。可以事先格式化好U盘，也可以在Web界面进行格式化。



1. 左侧勾选通道。在右侧设置查询条件，包括录像类型、文件类型和查询时间，点击<查询>。
2. （可选）点击[操作栏]中的按钮播放或备份某个文件。
3. 勾选需要备份的文件后，<备份>按钮右侧显示所需的备份空间。点击<备份>。
4. 在出现的窗口中设置备份任务及备份路径；还可以：
 - 创建新的文件夹。
 - 编辑、删除U盘上的文件和文件夹。
 - 将U盘格式化为NTFS或FAT32格式。
 - 查看U盘总容量和剩余容量。
5. 点击<确定>。
6. 点击页面右上角的<备份管理>按钮 () 查看备份任务或删除正在进行的备份任务。

6 系统配置

系统配置是对系统时间、假日、硬盘参数、网络等通用参数进行配置和维护。

支持基本配置、硬盘配置、网络配置、协议对接、安全配置、系统维护、主从切换和地图配置。

6.1 基本配置

包括设备基本信息、时间及时间同步、假日配置。

6.1.1 基本配置

系统配置>基本配置>基本配置

设置平台的设备名称、系统语言，查看产品型号、序列号、软件版本、视图库版本、运行时间等信息。

同步设备时间 开启 关闭

同步间隔 小时

同步设备时区 开启 关闭

保存

6.1.4 假日配置

系统配置>基本配置>假日配置

假日配置完成后，可以配合时间模板，在报警布防预案、录像计划等功能使用。更多信息请参考[时间模板](#)。

假日名称必须唯一。

假日配置 ×

*假日名称:

重复方式: 单次 常年

假日范围: 按日 按周

开始时间:

结束时间:

状态: 开启 关闭

确定

6.1.5 图像矫正

系统配置>基本配置>图像矫正

当上传的图片为多人时，识别其中完整人脸图片作为添加的图片，且可自动识别人脸，去除多余背景。

图像矫正默认开启，开启后可对以下场景中用户上传的图片进行自动矫正。

图像矫正 开启 关闭

保存

客户端类型	使用场景
C/S客户端	人脸识别、门禁管理
B/S客户端	人员管理
	 说明: 需下载WebAssist插件后才可进行自动矫正。

6.2 硬盘配置

管理平台、扩展柜或IPSAN的硬盘。

6.2.1 阵列配置

开启/关闭RAID模式；一键配置或手动创建RAID阵列。

系统配置>硬盘配置>阵列配置

开启/关闭RAID模式，创建阵列，查看阵列信息、配置热备盘、重建阵列等。

创建阵列

1. 开启RAID模式，点击<一键配置>或<手动创建>。

表 6-1: 一键配置和手动创建阵列

一键配置	手动创建
仅支持RAID1、RAID5	支持RAID0、RAID1、RAID5、RAID6、RAID10、RAID50、RAID60
自动命名阵列，格式为ARRAYn，如ARRAY1。	手动输入阵列名称（必须唯一）。
根据硬盘数自动选择阵列类型进行创建： <ul style="list-style-type: none"> • 2块盘：RAID1； • 3块盘：RAID5（无热备盘） • 4-8块盘：RAID5（1块热备盘） • 9-16块盘：2个RAID5（1块热备盘） 	<ul style="list-style-type: none"> • 手动配置阵列类型； • 对于RAID50、RAID60，还必须正确选择子阵列硬盘数及硬盘总数（所选硬盘总数必须为子阵列硬盘个数的整数倍，且倍数大于1）。
i 重要: <ul style="list-style-type: none"> • 创建阵列时会自动格式化硬盘。 • 热备盘为磁盘中容量最大的一块；若多块盘容量一样大，取最后一块作为热备盘。 • 创建2个RAID5时，若磁盘总数为奇数（N），则两个RAID5中的磁盘数均为$(N-1)/2$；若磁盘总数为偶数，则两个RAID5中的磁盘数分别为$N/2$和$N/2-1$。 • 用于创建一个阵列的硬盘只能全部来自同一台设备：平台或扩展柜（若有连接）；也就是说，不能使用平台和扩展柜A的硬盘创建一个阵列，也不能使用扩展柜A和扩展柜B的硬盘创建一个阵列。 	

表 6-2: 支持的RAID类型及对应硬盘数

RAID类型	硬盘数（块）
RAID0	2-8
RAID1	2
RAID5	3-8
RAID6	4-8
RAID10	4-16
RAID50	6-16
RAID60	8-16

2. 阵列创建完成后，在[物理硬盘]页签上查看阵列硬盘信息。点击[热备]列中的  将热备盘恢复成普通盘，点击  将普通盘设置为热备盘。

物理硬盘 阵列

提示：创建阵列所选的物理硬盘容量不一致，会造成硬盘空间浪费

 一键配置  手动创建

<input type="checkbox"/>	盘号	容量 (GB)	所属设备	类型	阵列	状态	热备
<input type="checkbox"/>	1	891	本地硬盘	热备盘		良好	

3. 点击[阵列]页签，查看已创建的阵列信息。

物理硬盘	阵列								
序号	所属设备	名称	总容量 (GB)	状态	类型	硬盘	热备	重建	删除
1	本地硬盘	ARRAY1	3725	正常	RAID5	1, 2, 3, 4, 5	11		
2	本地硬盘	ARRAY2	3725	正常	RAID5	6, 12, 13, 15, 16	11		

删除阵列

在[阵列]页签点击[删除列]中的删除阵列；阵列上的数据也将被一起删除。

重建阵列

当阵列中的某块硬盘发生故障时，若存在合适的热备盘（容量不小于阵列中最小硬盘的容量），阵列将在10分钟后自动进入重建状态。若没有合适的热备盘，需选择一块硬盘替代故障硬盘，手动重建阵列。注意所选硬盘的容量必须不小于阵列中容量最小的硬盘。

6.2.2 硬盘管理

系统配置>硬盘配置>硬盘管理

槽位信息	所属设备	状态	总容量 (GB)	剩余容量 (GB)	属性	盘组属性	所属服务器	操作
1	本地硬盘	正常	3685.77	3616.00	读写	普通存储	VMS-服务器-1	
8-1	IPSAN	正常	6666.00	6599.00	读写	IPSAN (S)	VMS-服务器-1	
2	本地硬盘	无硬盘	0.00	0.00	读写		VMS-服务器-1	

- 查看硬盘信息：槽位号、所属设备（本地硬盘或网络硬盘）、状态、容量使用情况等。

说明:

图片存储于槽位1的硬盘，请确认槽位1已安装硬盘且状态正常。

- 查看剩余存储天数：列表上方显示当前存储策略：若为“满即停”，则计算预计录像天数；若为“满覆盖”，计算覆盖周期（天）。
- 设置读写属性：在属性列下拉框选择“只读”/“读写”；或勾选硬盘，点击列表上方<只读>/<读写>。
- 设置盘组属性：在盘组属性下拉框选择“普通存储”/“备份存储”。
- 格式化：点击；或勾选硬盘，点击列表上方<格式化>。

说明:

- 在存在阵列时关闭RAID模式，硬盘状态显示为未格式化，必须手动格式化后才可以正常存储。
- 格式化将清空硬盘已存储的录像。

6.2.3 网络硬盘

系统配置>硬盘配置>网络硬盘

配置IPSAN。完成配置后，在[硬盘配置>容量配置]下分配IPSAN容量。

说明:

- 操作前，请先在IPSAN控制台上完成相关配置（如业务口IP地址）并创建Target和Initiator。
 - 小于2G的IPSAN资源，即使添加成功也无法正常使用。
1. 点击<添加>。在对话框中完成配置。

添加×

类型:

* IP:

* Target:

* Initiator:

用户名:

密码:

- IP：IPSAN的管理口或业务口的IP地址。与IPSAN控制台上的配置保持一致。
 - Initiator：IPSAN控制台上已创建好的Initiator。
 - Target：IPSAN控制台上已创建好的Target。
 - 用户名/密码：IPSAN鉴权用的用户名/密码。如果没有开启鉴权则不需要。
2. 点击<确定>保存。
 3. 可对已添加的IPSAN进行格式化、修改读写属性。

6.2.4 容量配置

系统配置>硬盘配置>容量配置

为IPC分配录像存储和抓图空间。可分配容量取决于[盘组属性](#)和[网络硬盘](#)中的配置。

 说明:

- 未分配固定容量的通道默认使用共享容量。
 - 若<分配容量>按钮灰显，请查看是否因为开启了RAID模式但未创建阵列。
1. 点击<分配容量>，选择通道，输入要分配的容量空间。

添加容量配置

通道

请输入关键字 🔍

- 206.9.252.2_V_13
- 206.9.252.2_V_24
- 206.9.252.2_V_31

普通容量: 5509GB 可分配容量: 5505GB

录像容量: GB

图片容量: GB

IPSAN容量: 0GB 可分配容量: 0GB

录像容量: GB

图片容量: GB

备份容量: 0GB 可分配容量: 0GB

录像容量: GB

确定
取消

- 普通容量：普通存储的容量。
 - IPSAN容量：分配IPSAN存储。
 - 备份容量：备份存储的容量。
 - 录像容量：用于存储录像。
 - 图片容量：用于存储联动抓图。
2. 容量分配结果出现在列表中。可点击 或 删除或修改。

6.2.5 盘组属性

系统配置>硬盘配置>盘组属性

1. 在[属性]列查看属性：
 - 普通存储：用于向IPC分配录像容量。
 - 备份存储：用于 **自动备份NVR** 上的录像。
 - IPSAN：已添加的网络硬盘。

盘组号 ⇅	容量 (GB) ⇅	属性 ⇅
1	0	普通存储

2. 在[容量]页签查看普通存储、备份存储和IPSAN的容量信息。
3. 在[硬盘配置>容量配置]下进行 [容量配置](#)。

6.2.6 高级配置

系统配置>硬盘配置>高级配置

配置平台上的录像存储满策略，即当平台硬盘存满之后所采用的相应操作：

- 满覆盖：默认模式。当平台硬盘存满时，覆盖之前的录像。优先覆盖时间最早的录像。
- 满即停：当平台硬盘存满时，停止保存录像。

满策略

- 满覆盖 当容量用完时覆盖最早的存储录像，继续存储。
- 满即停 未分配容量的通道，仍会被满覆盖，请分配具体容量。

说明:

只有在容量配置里分配了容量的情况下，满即停才有效，分配的容量用尽后停止存储。共享存储情况下，满即停配置不生效。

开启“UNP/云端设备开放存储功能”，能够实现跨广域网存储，可以对云端接入的设备进行中心存储。请阅读并同意免责声明后开启。

6.3 网络配置

6.3.1 TCP/IP

系统配置>网络配置>TCP/IP

对不同工作模式下的TCP/IP参数进行设置，包括IP地址获取方式（静态设定或DHCP获取）、IP地址、子网掩码、默认网关、MTU、首选和备选DNS服务器、默认路由等。

工作模式	<input type="text" value="多址设定"/>
网卡选择	<input type="text" value="网卡一"/>
DHCP	<input type="radio"/> 开启 <input checked="" type="radio"/> 关闭
IPv4地址	<input type="text" value="192.168.1.60"/>
IPv4子网掩码	<input type="text" value="255.255.255.0"/>
IPv4默认网关	<input type="text" value="192.168.1.1"/>
物理地址	<input type="text" value=""/>
MTU	<input type="text" value="1500"/>
连接状态	离线
速率	0kpbs
首选DNS服务器	<input type="text" value="192.168.2.230"/>
备选DNS服务器	<input type="text" value="8.8.8.8"/>
默认路由	<input type="text" value="网卡一"/>

保存

说明:

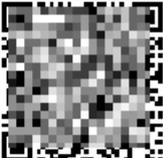
- 不同工作模式间的网络配置互不影响。
- 切换工作模式需重启设备并会清空自定义路由。
- 不同网卡的IPv4地址不能配置成属于相同网段。
- 工作模式

- 多址设定：默认模式。各网卡使用不同IP地址，各自独立工作。
- 负载均衡：组成虚拟网卡的网卡使用一个IP地址，同时工作，分担负载。
- 网络容错：组成虚拟网卡的网卡使用一个IP地址，相互备份。若其中一张网卡出现故障，则另一张网卡承担网络流量。
- DHCP：如果配置了DHCP服务器，可开启DHCP自动获取IP地址。
- IPv4地址：平台的网络地址。客户端通过该IP地址访问平台。
- 连接状态：所选网卡的连接状态。当对应网口插上网线并连接正常时，状态为“在线”。
- DNS服务器：域名解析服务器，将域名解析为IP地址。
- 默认路由：指设备发送数据时默认选择通过哪张网卡发送。默认路由所选的网卡可以和[网卡选择]下拉框中的网卡不同，最终以默认路由选择的网卡为准。

6.3.2 宇视云

系统配置>网络配置>宇视云

宇视云用于远程监控业务，默认关闭。启用后，使用注册码将平台注册到宇视云网站。如果设备状态显示为在线，可以通过云账号登录平台（参见《综合监控一体化平台软件客户端用户手册》的“登录”章节）。

宇视云	<input checked="" type="radio"/> 开启 <input type="radio"/> 关闭
服务器地址	ezcloud.uniview.com
注册码	XXXXXXXXXXXXXXXXXXXX
设备状态	在线 <input type="button" value="注销"/>
用户名	f00432
设备名称	vm52-7-8
服务协议	http://ezcloud.uniview.com/doc/termsofservice.html
设备网络类型检测	<input type="button" value="检测"/>
扫一扫	

- 注册码：每台平台服务器都有一个唯一的注册码，用于将平台添加至云端。
- 设备状态：如果显示在线，则可以通过云账号登录平台；如果点击<注销>，平台将从云端删除。
- 用户名：注册平台时使用的云网站的用户名。
- 设备名称：平台的云端名称。
- 设备网络类型检测：点击检测平台所处网络的NAT类型、IP地址类型、防火墙。
- 扫一扫：使用手机客户端扫描二维码将平台添加至云端。



说明:

平台支持接入宇视云，支持添加云端IPC/NVR，以及通过电脑客户端和EZView远程访问。为保证体验，建议平台设备直连公网，即具备公网IP或者能够通过单层端口映射连接到公网。

6.3.3 DDNS

系统配置>网络配置>DDNS

DDNS是动态域名服务，用来将动态的IP地址绑定到固定的域名上，使用户可以通过域名访问平台。[点击此处了解什么是DDNS。](#)

DDNS默认关闭。启用后可对服务进行具体配置。当前支持3种类型的DDNS服务：DynDNS、NO-IP、EZDDNS。

- DynDNS：使用前，用户需在DynDNS官网完成注册。完成注册后，在页面上输入服务器地址、端口号、域名、以及认证用的用户名和密码。配置成功后，设备状态显示为在线，可使用域名访问平台。
- No-IP：使用前，用户需在No-IP官网注册账号。完成注册后，在页面上输入服务器地址、端口号、域名、以及认证用的用户名和密码。配置成功后，设备状态显示为在线，可使用域名访问平台。
- EZDDNS：
 - 默认服务器地址：ezcloud.uniview.com。
 - 默认端口：80。
 - 域名：输入域名后（如VMS2），点击<域名检测>，检测域名是否可用。检测成功后，点击<保存>。如果设备状态显示为在线，则可使用生成的设备地址（如ezcloud.uniview.com/vms2访问平台。）

6.3.4 端口

系统配置>网络配置>端口

配置HTTP、HTTPS、RTSP、报警端口。

HTTP端口	<input type="text" value="80"/>
HTTPS端口	<input type="text" value="443"/>
RTSP端口	<input type="text" value="554"/>
报警端口	<input type="text" value="52075"/>

注意：修改HTTP端口后，请重新登录。

保存

6.3.5 端口映射

系统配置>网络配置>端口映射

配置端口映射，将平台公网地址的外部端口映射到私网地址的内部端口，达到通过访问该外部端口就能访问内部端口的目的。平台支持两种端口映射方式：

- UPnP：
 - 自动协商：平台和路由器自动协商外部端口号。如果一个端口被占用，平台会随机选用其他端口发起映射请求，确保端口可用。
 - 指定端口：指定外部端口号。如果指定端口被占用，平台不会尝试用别的端口进行映射。
- 手动映射：路由器不支持UPnP时使用该模式。先在路由器上完成配置，然后填入本页面。

 说明:

- 端口映射默认关闭。
- 在设置UPnP功能前，需要先在路由器中启用UPnP。

6.3.6 自定义路由

系统配置>网络配置>自定义路由

添加平台的静态路由，实现平台与目的网段的互通。最多允许100条自定义路由。

添加时需指定网卡并设置IP网段、子网掩码以及网关。添加的路由处于开启状态，可以手动关闭。

添加 ×

状态: 开启 关闭

网卡:

*IP网段:

*子网掩码:

*网关:



说明:

切换网卡的工作模式会清空所有自定义路由。

6.3.7 邮件

系统配置>网络配置>邮件

用户可以通过邮件配置，配置联动邮件的发件人信息以及SMTP服务器。配置完成后，可在报警布防联动等功能模块使用邮件功能。

服务器认证 开启 关闭

用户名

密码

SMTP服务器

SMTP端口 启用TLS/SSL

发件人名称

发件人地址



说明:

- 开启 (SMTP) 服务器认证功能后，需要输入正确的用户名和密码。
- 启用TLS/SSL后，平台与SMTP服务器之间的数据将被加密。
- 启用TLS/SSL功能可能需要相应修改SMTP端口。

6.3.8 AD域配置

系统配置>网络配置>AD域配置

配置以下参数，将系统接入AD域，以实现统一管理和权限控制。

域名	<input type="text"/>
主机名	<input type="text"/>
端口	<input type="text" value="636"/>
启用SSL	<input checked="" type="radio"/> 开启 <input type="radio"/> 关闭
名称	<input type="text"/>
密码	<input type="text"/>
基准DN	<input type="text" value=""/> <input type="button" value="获取DN"/>

6.4 协议对接

6.4.1 UNP

术语介绍

- UNP (Universal Network Passport)，即万能网络护照，是宇视独有的专利技术，使监控系统可以穿越防火墙和NAT设备，在上下级域或设备与平台之间建立专有通道，简化网络监控。
- UNP服务器：当平台作为UNP服务器时需要配置。完成配置后，平台作为UNP服务器，接入NVR、IPC等设备。
- UNP客户端：当平台作为UNP客户端接入到上级管理平台（如VM）时需要配置。完成配置后，平台作为UNP客户端，接入到上级管理平台。

说明:

- UNP客户端和UNP服务器不能同时开启。
- 可在平台网页客户端的登录页下载UNP客户端。
- 当平台作为UNP服务器接入设备（如NVR）时，还需在接入设备中完成UNP客户端配置。
- 当平台作为UNP客户端接入到上级管理平台（如VM）时，还需在上级管理平台中完成UNP服务器配置。
- 当平台作为UNP服务器时，需要在路由器上作端口配置，将平台的1701端口映射到公网，其公网映射端口也必须是1701。如果接入UNP2.0的客户端，还需映射5555端口。

UNP客户端

系统配置>协议对接>UNP>UNP客户端

当平台作为UNP客户端接入到上级管理平台（如VM）时需要配置。

UNP 客户端 开启 关闭

UNP模式 UNP1.0

服务器地址 192.168.2.1

服务器端口 80

用户验证 开启 关闭

用户名

密码

保存

部分参数解释如下。

- UNP客户端：开启或关闭平台的UNP客户端配置（默认关闭）。
- UNP模式：UNP1.0或UNP2.0。
- 服务器地址：UNP服务器的IP地址。
- 服务器端口：UNP服务器的端口号。
- 加密：UNP2.0时，是否对UNP客户端与UNP服务器之间的报文进行加密。加密能提高安全性，但会占用一定带宽。
- 用户名/密码：必须与UNP服务器上设置的一致。
- IP地址、子网掩码、网关：UNP客户端自动获取的IP地址、子网掩码和网关。

UNP服务器

系统配置>协议对接>UNP>UNP服务器

当平台作为UNP服务器接入NVR等设备时需要配置。

UNP 服务器 开启 关闭

动态分配IP地址 10.10.10.100

动态分配子网掩码 255.255.255.0

UNP客户端虚拟地址池 10.10.10.2 - 10.10.10.253 地址池应避免包含任何编码设备的IP地址，否则可能影响录像计划的配置。

UNP服务器虚拟地址 10.10.10.1

UNP服务器端口 1701,5555

用户名 admin

密码

保存

连接状态 刷新

IP地址 已接收 (包数) 已发送 (包数)

部分参数解释如下。

- UNP服务器：开启或关闭平台的UNP服务器配置（默认关闭）。
- 动态分配IP地址：UNP服务器给客户端分配IP的地址段。
- 动态分配子网掩码：UNP服务器给客户端分配IP的地址段的子网掩码。
- UNP客户端虚拟地址池：UNP服务器给客户端分配的虚拟IP地址池；根据“动态分配IP地址”及“动态分配子网掩码”自动生成。
- UNP服务器虚拟地址：UNP服务器自身的虚拟地址，默认为动态分配IP地址段中的第一个IP地址。
- UNP服务器端口：UNP服务器使用的端口号。
- 用户名/密码：接入UNP服务器时鉴权使用。

- 连接状态：查看UNP服务器与UNP客户端之间的连接状态。

说明:

配置“UNP客户端虚拟地址池”时应注意避免包含编码设备的IP地址。具体影响如下：

- 在UNP服务开启时添加编码设备，如果编码设备的IP地址在虚拟地址池范围内，那么编码设备将被视为UNP设备，不能配置录像计划。
- 在UNP服务关闭时添加编码设备，即使编码设备的IP地址在虚拟地址池范围内，编码设备也不会被视为UNP设备，不会影响录像计划的配置。
- 对于已经添加为UNP设备的编码设备，即使关闭了UNP服务，编码设备也会保持当前的UNP设备属性，直到平台重启。

6.4.2 国标

国标服务器配置

系统配置>协议对接>国标>国标服务器配置

完成国标服务器配置，用国标协议（GB/T28181）将平台服务器接入上级管理平台，实现对平台服务器的统一管理，在上级管理平台上对平台下的通道进行实况、回放和报警订阅等操作。

在国标服务器配置中，SIP服务器指上级管理平台服务器。

- 完成基本配置

- SIP服务器编码：上级管理平台服务器编码（从上级平台服务器获取）。
- SIP服务器IP：上级管理平台服务器的IP地址（从上级平台服务器获取）。
- 组织：显示基本组织及所有自定义组织。切换组织后需点击<保存>，左下角的组织树显示所选组织。
- SIP域：上级管理平台服务器的域名编码。
- SIP服务器端口：上级管理平台服务器的端口号。
- 心跳周期：平台与上级管理平台之间的保活时间。
- 最大心跳超时次数：统计平台与上级管理平台服务器之间通信超时次数。一旦超过设定的最大次数，通信将自动断开。
- 将通道共享给上级管理平台
共享成功的通道可以在上级管理平台的操作界面查询到，并能进行报警订阅等操作。未共享的通道不能在上级管理平台查询到。取消共享的通道将在上级平台被直接删除。

1. 从[组织]下拉框选择组织，然后点击<保存>。组织树上显示所选组织。
2. 在左侧选择待共享的通道类型：视频通道、报警输入通道或音频通道。
3. 在组织树上编辑组织编码。可勾选组织，然后点击<批量编辑>按钮（图中1）进行批量操作。
4. 配置通道编码有以下两种方式。

- 单个配置：单击对应通道操作列下的 ，输入通道编码。
 - 批量编辑：勾选需要配置的通道，单击<快速配置>按钮（图中2），设置基准编码，系统将在基准编码基础上自动依次生成编码并分配给各通道，仅对通道编码为空的通道生效。
5. 可勾选通道，然后点击<批量编辑>按钮（图中3），批量修改通道编码。

 说明:

- 通道编码格式为8位中心编码+2位行业编码+3位类型编码+7位序号。
 - 基准编码是新增通道编码的起始编码，系统在基准编码基础上依次生成编码并分配给通道。设置基准编码时，第一段10位为默认值，允许修改；第二段根据通道类型自行选择；第3段为序号，需要用户设定。
 - 快速配置功能仅对通道编码为空的通道有效，不会改变已有编码。
 - 在组织树上修改组织编码时，注意组织编码必须在本域内唯一，不能与其他组织或通道编码相同。
6. 分配了编码的通道默认处于“已共享”状态，在上级平台上可以查询到这些通道并进行报警订阅，接收共享通道的报警订阅消息。
7. 要取消通道共享，选择通道，点击<取消共享>。共享取消后，通道状态变为“未共享”。取消共享的通道在上级平台被直接删除。

 说明:

音频通道无法主动共享或取消共享。音频通道的共享状态与对应的视频通道的共享状态保持一致。共享某个视频通道将同时共享其对应的音频通道；取消共享也一样。

国标本地配置

系统配置>协议对接>国标>国标本地配置

完成国标本地配置，用国标协议（GB/T28181）将下行设备（如IPC和NVR）接入平台。在国标本地配置中，SIP服务器指平台。

- SIP服务器编码：平台的国标编码。
- SIP服务器端口：平台的国标端口号。
- 心跳周期：下行设备（IPC、NVR等）与平台之间的保活时间。
- 最大心跳超时次数：统计下行设备与平台之间通信超时次数。一旦超过设定的最大次数，通信将自动断开。

SIP服务器编码	34020000002001300023
SIP服务器端口	5063
心跳周期（秒）	60
最大心跳超时次数	3

保存

6.4.3 视图库

系统配置>协议对接>视图库

视图库GA/T1400配置包括服务器配置和本地配置。

视图库GA/T1400服务器配置

视图库GA/T1400服务器配置 开启 关闭

设备状态 **在线**

上级视图库IP 上级视图库端口

用户名 密码

- 设备状态：平台成功连接视图库服务器时显示为“在线”。
- 上级视图库IP：视图库服务器的IP地址。
- 上级视图库端口：视图库服务器上开放的端口号。
- 用户名/密码：平台接入视图库服务器的用户名和密码。

视图库GA/T1400本地配置

本地编码 格式8位中心编码+2位行业编码+3位类型编码+7位序号，共20位（序号必须为数字，其余为数字或字母）

本地端口

- 本地编码：平台自身的视图库编码，用于平台向上级视图库注册时标识自身身份。
- 本地端口：5073。平台提供给下级设备的连接端口。需要在下级设备上配置此端口。

添加采集设备/视频卡口/采集系统，将下行设备接入平台。

已添加的设备通道可以在上级管理平台的操作界面查询到，并能进行报警订阅等操作。

采集设备 视频卡口 采集系统

视图库接入的设备和通道不能删除。

<input type="checkbox"/>	通道名称	设备编码	位置名	管辖单位代码	经度	纬度	操作
<input type="checkbox"/>	192.168.1.141_V_1	1234567891011121314151617181920	XX		0	0	<input type="button" value="编辑"/> <input type="button" value="删除"/>

添加采集设备/视频卡口/采集系统的方式类似，此处以采集设备为例。

1. 单击<添加>。

添加

通道

Q 请输入关键字

- root
- 192.168.1.141_V_1

设备编码:

位置名:

管辖单位代码:

经度:

纬度:

- 启用计划1/2：启用后，在指定时间点完成一次抓图并上传；如果同时启用，两个指定时间点的间隔不能小于5秒。
- 随机启用：启用后，每隔5分钟上传一次抓图。
- 报修：上报故障，如视频丢失、图像异常等。
- 维保：上报维护结果（如已修复、未修复）。
- 手动抓图：选择通道，手动抓图上传。

2. 点击<保存>。

6.5 安全配置

6.5.1 802.1x

系统配置>安全配置>802.1x

802.1x协议是一种基于端口的网络接入控制协议，连接在端口上的用户设备必须先通过认证才能访问局域网中的资源。

- 可选择网卡启用802.1x认证配置。不同网卡的认证信息互相独立。若网卡工作模式为负载均衡或网络容错，则显示网卡绑定1和网卡绑定2。
- 协议类型：当前仅支持EAP-MD5。
- EAPOL版本号：1表示802.1x-2001，2表示802.1x-2004。
- 用户名和密码：用于认证。只有输入的用户名和密码同认证设备（如交换机）上设置的相同才能通过认证。

网卡选择	<input type="text" value="网卡一"/>
802.1x	<input checked="" type="radio"/> 开启 <input type="radio"/> 关闭
协议类型	<input type="text" value="EAP-MD5"/>
EAPOL版本	<input type="text" value="1"/>
用户名	<input type="text" value="admin"/>
密码	<input type="password" value="*****"/>

保存



说明：

需要同时在认证设备（如交换机）上配置相应的802.1x认证才能生效。

6.5.2 ARP攻击

系统配置>安全配置>ARP防攻击

通过将平台的网卡的IP地址与网卡的MAC地址绑定，防止因为网关MAC地址被恶意篡改而导致平台与局域网外的通信中断。

可自动获取或手动设置网关的MAC地址。

网卡选择

ARP防攻击 开启 关闭

网关

网关物理地址 自动获取 🔔 切换到自动获取MAC地址存在被攻击风险

保存

说明:
在发生ARP攻击前开启该功能，保护才生效；在受到攻击时改变网关MAC地址绑定，保护可能失效。

6.5.3 HTTPS

系统配置>安全配置>HTTPS

HTTPS (安全超文本传输协议) 是一种安全的通信方式，通过安全套接层 (SSL) 或传输层安全 (TLS) 连接发送HTTP，对HTTP和数据本身进行加密。支持通过创建私有证书或上传已签名证书以开启HTTPS功能。

- 私有证书：未经过权威机构认证的、私人创建的证书。
- 证书请求：使用受信任的公司颁发的证书。

创建证书并开启HTTPS功能后，可使用“https://设备IP”的方式访问设备。

说明:

- 私有证书创建成功后，必须先删除原有证书才能创建新证书。
- 证书请求创建成功后，必须先删除原有证书请求才能创建新请求。
- HTTPS功能开启时无法删除证书，必须先关闭HTTPS功能并点击<保存>。

6.5.4 SSH

系统配置>安全配置>SSH

默认关闭SSH，开启后可通过SSH远程登录平台。

SSH 开启 关闭

保存

6.5.5 IP地址过滤

系统配置>安全配置>IP地址过滤

通过配置黑/白名单，禁止或只允许特定IP地址的客户端PC访问平台。

IP地址过滤 关闭 黑名单 白名单

IP地址 **添加**

起始IP地址	结束IP地址	操作
192.167.2.55	192.167.2.255	

- 黑名单：开启时，禁止指定IP地址的PC访问平台。
- 白名单：开启时，只允许特定IP地址的PC访问平台。

说明:

- 黑白名单不能同时开启。
- 黑白名单控制只对IP地址登录有效。
- 可双击规则列表中的IP地址进行编辑。

6.6 系统维护

6.6.1 系统维护

系统配置>系统维护>系统维护

对平台进行重启、恢复默认配置、导出和导入配置、导出诊断信息以及本地升级等操作。

重启	重新启动设备
简单恢复	保留网络配置、用户配置和事件配置
完全恢复	恢复设备参数到出厂设置
导出配置	导出配置文件
导入配置	<input type="text"/>  <input type="button" value="导入"/>
本地升级	<input type="text"/>  <input type="button" value="升级"/>
控件日志路径	<input type="text" value="C:\Users\Administrator\AppData\Local\Temp\..."/>  <input type="button" value="打开文件夹"/>
导出诊断信息:	
所属服务器	<input type="text" value="VMS ..."/> <input type="button" value="导出诊断信息"/>

- 简单恢复：恢复除网络、用户、事件以外的其他配置。注：会保留[安全配置]页签下除IP地址过滤之外的所有配置项。
- 完全恢复：将所有配置恢复成出厂设置。
- 导出配置：导出当前配置并保存为文件，以便将来需要时通过导入该备份文件恢复配置。
- 导入配置：通过导入备份配置文件恢复平台配置。平台将重启。
- 本地升级：使用本地升级文件升级平台的版本。
- 控件日志路径：点击<打开文件夹>查看控件日志。点击文件夹图标 ()，可以自定义路径。当未安装控件或浏览器不支持控件时，输入框和按钮都灰显不可用。
- 导出诊断信息：导出平台的诊断信息。

6.6.2 设备诊断信息

系统配置>系统维护>设备诊断信息

导出与平台直连的设备 (IPC和NVR) 的诊断信息，包括实时诊断信息和历史诊断信息。点击 导出。只有当设备在线时可导出实时诊断信息。

实时诊断信息		历史诊断信息			
文件保存路径: <input type="text"/> <input type="button" value="打开文件夹"/>		导出诊断信息 <input type="text" value="请输入关键字"/>			
设备名称	所属服务器	所属组织	设备型号	在线状态	操作
192.168.2.38	VMS	root	EDU	<input checked="" type="checkbox"/> 在线	<input type="button" value="导出"/>

导出历史诊断信息需NVR在线（离线的IPC仍可导出）。最多可导出最近15天的诊断信息。

实时诊断信息		历史诊断信息			
请输入关键字 <input type="text"/>					
设备名称	所属服务器	所属组织	设备型号	在线状态	操作
192.168.2.38	VMS	root	EDU	<input checked="" type="checkbox"/> 在线	<input type="button" value="导出"/>

 **说明:**
 国标设备和第三方设备不支持诊断信息导出。

6.6.3 日志清理

系统配置>系统维护>日志清理

设置日志的最长保留天数。超过设定天数的日志将被自动删除。默认最长保存时间为30天。

操作日志	最长保留	<input type="text" value="30"/>	天 (0表示不清理)
报警日志	最长保留	<input type="text" value="30"/>	天 (0表示不清理)
门禁出入记录	最长保留	<input type="text" value="30"/>	天 (0表示不清理)

6.6.4 网络抓包

系统配置>系统维护>网络抓包

抓包用于问题分析和定位。可设定条件（端口号、IP地址、网卡和数据包大小）抓取或过滤指定端口和/或IP地址的数据包。

设定完条件后，点击<创建抓包任务>。最多可创建5个任务。创建的任务出现在列表中。可点击删除抓包任务。

点击开始执行任务，点击停止，然后点击将数据导出至本地。每完成一个任务后手动进行一次导出操作。

端口	<input checked="" type="radio"/> 全部 <input type="radio"/> 指定 <input type="radio"/> 过滤
IP地址	<input checked="" type="radio"/> 全部 <input type="radio"/> 指定 <input type="radio"/> 过滤
网卡选择	<input type="text" value="网卡一"/> 192.168.1.60
数据包大小 (字节)	<input type="text" value="8192"/>
<input type="button" value="创建抓包任务"/> 最多创建 5 个抓包任务	

任务	状态	操作
101_eth1_SPECIFY_192.168.2.109_FILTER_554	完成	<input type="button" value="删除"/> <input type="button" value="导出"/>
102_eth1_SPECIFY_192.168.4.16_FILTER_554	完成	<input type="button" value="删除"/> <input type="button" value="导出"/>

 **说明:**

- 上图中，抓包任务名中的SPECIFY表示指定，FILTER表示过滤。
- 抓包过程中会生成抓包文件。单个抓包文件大小有限制（最大约19.1M）。当文件大小达到限制时，对应的抓包任务自动停止（注意：自动停止后，界面上的状态不会自动更新，依旧是“进行中”）。

6.6.5 网络检测

系统配置>系统维护>网络检测

输入域名或IP地址，点击<开始检测>。通过检测结果确定网络是否连通，以及连通状态下的时延和丢包率。

检测地址	<input type="text" value="192.168.2.1"/>	<input type="button" value="开始检测"/>
检测结果	延时: 0.501毫秒, 丢包率: 0%	

6.6.6 网络资源统计

系统配置>系统维护>网络资源统计

显示平台的网络带宽使用数据。带宽数据约每5秒钟刷新一次。

类型	带宽
IP通道接入	0Kbps
远程回放接入	0Kbps
远程预览	0Kbps
远程回放及下载	0Kbps
网络接收剩余	512Mbps
网络发送剩余	384Mbps

当接入带宽被全部占用（网络接收剩余为0）时，会出现媒体流异常等现象。

- IP通道接入：平台从设备（如IPC、NVR）接收实况流时的带宽使用情况。
- 远程回放接入：平台从设备（NVR）接收回放流时的带宽使用情况（比如当客户端上播放NVR上的录像时）。
- 远程预览：平台发送实况流所使用的带宽（比如当在客户端或电视墙上播放实况时）。
- 远程回放及下载：平台发送回放流所使用的带宽（比如当在客户端或电视墙上进行回放、或者当录像下载时）。

6.6.7 媒体流传输策略

系统配置>系统维护>媒体流传输策略

“直连优先”策略仅在局域网内有效，并且需要与我司下行设备（IPC、NVR）配套使用。当“媒体流传输策略”设置为“直连优先”时，平台在建立媒体流业务时会根据下行设备的当前剩余发送带宽，选择采用转发或者直连。若直连条件满足，媒体流从下行设备直接发送至解码器，从而节省平台的转发性能消耗；若直连条件不满足，媒体流还是通过平台转发。

当设置为转发优先时，媒体流直接通过平台转发。

添加
✕

设备

- 根组织
- 192.168.2.124

媒体流传输策略: 直连优先

媒体流传输协议: TCP UDP

注: 部分解码器不支持TCP直连。

确定
取消

说明:
部分解码器不支持TCP直连；即使在界面上完成了配置，但实际不生效。

6.6.8 数据备份

系统配置>系统维护>数据备份

备份平台数据库，以便在需要通过备份的数据库快速恢复平台配置。

参数配置
备份记录
运维统计备份
运维统计备份记录

定期备份 开启 关闭

备份周期 天

备份频率 1 天, 多少天备份一次

备份时间 🕒 00:00

备份文件数量 - 30 + 备份文件最多存放份数

手动备份
保存

配置定期备份

在[参数配置]页签下配置定期备份，使平台根据设定的周期、频率和时间自动备份数据库。

- 定期备份：开启后可配置定期备份。
- 备份周期：可选择以天、周、月为周期进行备份。
 - 备份周期为“天”时：设置备份频率，即多少天备份一次。
 - 备份周期为“周”时：选择每周星期几（可多选）进行备份。
 - 备份周期为“月”时：选择每月几号（可多选）进行备份。
- 备份时间：备份操作的执行时间。

- 备份文件数量：最多存放多少份备份文件。最大支持30份备份。达到上限后，新备份会覆盖老备份。

手动备份

在[参数配置]页签下，点击<手动备份>。[备份记录]页签下出现相应的备份记录。

查看备份记录

在[备份记录]页签下查看定时备份和手动备份的备份记录。可点击[操作]列中的，导出备份文件。

使用备份数据还原

在[备份记录]页签下，选定某条备份记录，点击[操作]列中的，使用该备份记录还原系统。界面提示“还原操作将重启系统”。点击<确定>继续。

备份运维统计数据

通过任务自动备份运维统计数据。

在[运维统计备份]页签下点击<添加>创建任务。设置周期备份、备份频率和备份时间（请参见[配置定期备份](#)）。可选择设备类型（如编码设备、解码设备）、设备状态（在线、离线等）、导出类型（设备或通道）。添加接收定时备份文件的收件人。若发送失败，[运维统计备份记录]页签下会生成相应的失败记录（发送成功则没有记录），可选择一条或多条记录进行导出。

6.6.9 一键收集

1. 选择收集天数。
2. 单击<一键收集>收集设备日志等信息。

收集天数

收集信息包括：设备表、通道表、驱动表、带宽表、设备告警日志表、服务器告警日志表、操作日志表、在线用户信息表、日志压缩包

[一键收集](#)

6.7 主从切换

系统配置>主从切换>主从切换

- 配置从机，扩展存储和转发性能。主从机之间可以相互切换；可以改变从机挂载的主机。



注意：

主从模式下，主机性能下降一半。从机超过3台时，主机只做管理。

- 配置双机热备，提高系统可靠性。

6.7.1 主机切换为从机



说明：

- 添加从机时在从机上操作（切换为从机后输入主机的IP地址）。
- 主从机的软件版本不匹配时，需要先将主机或从机升级为匹配版本。
- 主从切换时，数据将被清空，平台将重启，密码恢复成默认密码。
- 支持的从机数有上限。达到上限后，不能继续添加从机。
- 不能从软件客户端登录从机。

1. 选择[从机]，输入要注册的主机的IP地址。
2. 单击<一键检测>可检测主机IP是否可用和主从机版本是否一致，下方将展示检测结果。

主从切换 主机 从机 主机IP地址 192 . 168 . 3 . 155 一键检测

成功

保存

3. 检测成功后，单击<保存>即可进行切换。切换成功后，从机状态显示为在线。

6.7.2 从机切换为主机

选择[主机]，点击<保存>。

6.7.3 更换主机

选择[从机]，输入新主机的IP地址，点击<保存>。

6.7.4 热备配置

指定中心服务器的工作模式。

说明:

- 只需在一台服务器（主机或备机）上完成双机热备配置。
- 开启双机热备后，备机Web界面上的一些配置、功能将被屏蔽或无法使用；不能从软件客户端登录备机。
- 主机配有录像计划时，若发生宕机并恢复后，备机上的录像将自动回迁至主机。为确保业务稳定，建议在设备宕机后尽快恢复。
- 当主机下挂有从机并启用热备，要保证主从连接正常，必须在从机的网页客户端（见TCP/IP）将主机IP修改为虚拟IP。
- 切换从机需先关闭热备模式。

主从切换 主机 从机

开启热备 开启 关闭

热备配置

角色

虚拟IP 说明：同网段中未使用的IP地址。

子网掩码

虚拟路由ID 说明：配置有多套双机热备时必须唯一。

备机业务IP

备机心跳IP 一键检测

报警和操作日志数据 清除

保存

1. 选择[主机]，选择[开启]热备。参照以下说明进行设置（以主机工作模式为例）。

- 角色：主机为“工作模式”，备机为“备份模式”。
- 虚拟IP：选择一个网络中未使用的IP地址。完成配置后，使用虚拟IP地址登录网页和软件客户端。
- 虚拟路由ID：用于区分网络中的两套双机热备；必须唯一。

- 备机业务IP：备机的IPv4地址（见TCP/IP）。
 - 备机心跳IP：同备机业务IP地址。用于主备机之间的心跳检测。如果在一定时间内没有检测到主机的心跳，备机自动切换成主机工作模式。
 - 一键检测：检测配置是否有效。检测成功才可以保存配置。
 - 报警和操作日志数据：勾选[清除]有助于加快主备机之间的同步速度。
2. 完成配置并检测成功后，点击<保存>。

6.8 地图配置

系统配置>地图配置

- 选择<图片地图>，在软件客户端[电子地图]中，手动添加图片作为地图。
- 选择<在线地图>，在软件客户端[电子地图]中，[地图应用]和[地图配置]页签下默认出现“高德地图”。可设置经度、纬度、初始缩放级别。

6.9 组件管理

系统配置>组件管理>考勤服务

单击<安装>。安装考勤服务组件后，支持在平台设置班次并为人员进行排班、请假、补签等操作，一站式**管理人员考勤**。

考勤服务

安装

 说明:

- 安装完成后可设置门禁设备测量通过人员的温度单位。
- 20A16-DT型号的服务器不支持安装考勤服务组件。

7 视频应用

视频应用是对视频参数和文件格式进行配置，查看相机的实况、回放。

通过视频应用功能，可远程查看设备所拍摄的实时画面、在异常事件发生后调取录像文件，代替人力现场巡逻，及时感知异常状况。

支持查看实况、回放和进行本地配置。

在网页客户端上查看实况和播放录像。您可能需要根据页面提示，下载并安装最新版本的控件。

 说明:

未安装控件的情况下仍可以播放H.264格式的实况，但会隐藏 [回放]及[本地配置]页面。

7.1 实况

视频应用>实况

启动实况

- 双击在线摄像机，或将摄像机拖至窗格启动实况。
- 拖拽组织或NVR设备节点至任意窗格启动实况。当所选摄像机数大于当前窗格数时，会自动切换分屏。

说明:

- 启动实况后，摄像机图标发生变化，如从  变为 。
- 单击播放窗格，对应摄像机在通道列表中高亮显示（如  206.9.252.15_V_01 ）。
- 切换页面后，实况自动停止。

实况操作

实况过程中使用底部工具栏操作。工具栏上的部分按钮仅对当前选中窗格有效。工具栏上的按钮可能因摄像机而异。



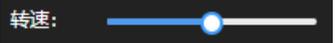
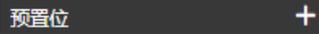
序号	描述
A	切换分屏，最多25分屏。
B	关闭所有窗格的实况。
C	当前窗格的视频帧率、码率、分辨率、编码格式、丢包率（图中为示例）。
D	抓取当前视频画面并保存至本地。保存路径在本地配置中设置。
E	点击后开始本地录像，点击  停止。保存路径在本地配置中设置。
F	数字放大。启用后，按住鼠标左键在画面上拉框，放大指定区域，然后使用鼠标滚轮放大或缩小画面。单击  关闭。
G	调节PC侧的音量输出大小或静音。
H	调节视频参数，包括亮度、饱和度、对比度、锐度。
I	选择码流类型：主流、辅流、第三流 说明: 实际支持的码流类型与摄像机有关。码流类型为不支持的视频流格式（如MJPEG）时不显示。
J	调整播放比例：满比例或按比例。
K	全屏。也可以按Esc键退出全屏。

对云台摄像机，点击窗格右侧按钮（  ）将展开云台控制面板，进行云台控制操作。

说明:

- 只有对支持并配置云台的摄像机才能进行云台控制操作；实际有效的云台控制操作取决于云台摄像机本身支持的功能和云台协议。
- GB协议接入的云台相机不支持照明和除雪功能。

按钮	描述
	锁定/解锁云台，锁定后非admin用户将不可操作云台任何功能，对admin用户操作无影响。 说明: 仅admin用户可锁定或解锁云台。

按钮	描述
	点击方向键，控制云台的转动方向 说明： 您也可以将鼠标光标放置在播放窗格中靠近窗格边缘的位置，点击鼠标左键转动一定角度，或者按住鼠标一直转动。
	调整镜头的焦距，使图像更加清晰。
	调整镜头变倍，放大、缩小图像。 说明： 还可以先点击播放画面的任意位置，然后通过鼠标滚轮进行变倍。
	调整镜头光圈。
	调整云台转速。
	设置预置位： <ul style="list-style-type: none"> ：点击添加预置位，即根据当前的云台状态将该位置添加到预置位列表中。 ：点击转到选中预置位。 ：删除预置位。 说明： 添加预置位时，注意编号不要与已有编号重复，否则将替换原有的预置位。
	开启/关闭照明。
	开启/关闭雨刷。
	开启/关闭红外。
	开启/关闭加热。
	开启/关闭除雪模式。

停止实况

- 点击窗格右上角的 。
- 点击工具栏中的  将关闭所有实况。
- 切换页面后，实况自动停止。

7.2 回放

视频应用>回放

术语介绍

- 中心录像：保存在平台上的录像。
- 设备录像：保存在NVR上的录像。
- 备份录像：指按计划自动从NVR备份到平台上的录像。

- 视频通道：一个视频通道对应一台摄像机。
- 普通录像：通过录像计划保存的录像。
- 事件录像：由事件（如报警）触发的录像段。

录像查询

1. 点击选择录像源。
2. 勾选摄像机（最多16台）。可输入关键字进行过滤。
日历上显示当月的录像情况：蓝色表示存在普通录像，红色表示存在事件录像；没有录像则不显示（如下图）。



3. 点击选择一个有录像的日期。
4. 点击<查询>。

查询结果显示在时间轴（进度条）和右侧文件列表中。不同类型的录像以不同颜色显示在时间轴上：蓝色表示普通录像（计划），红色表示事件录像（报警）（见[回放控制](#)）。

说明:

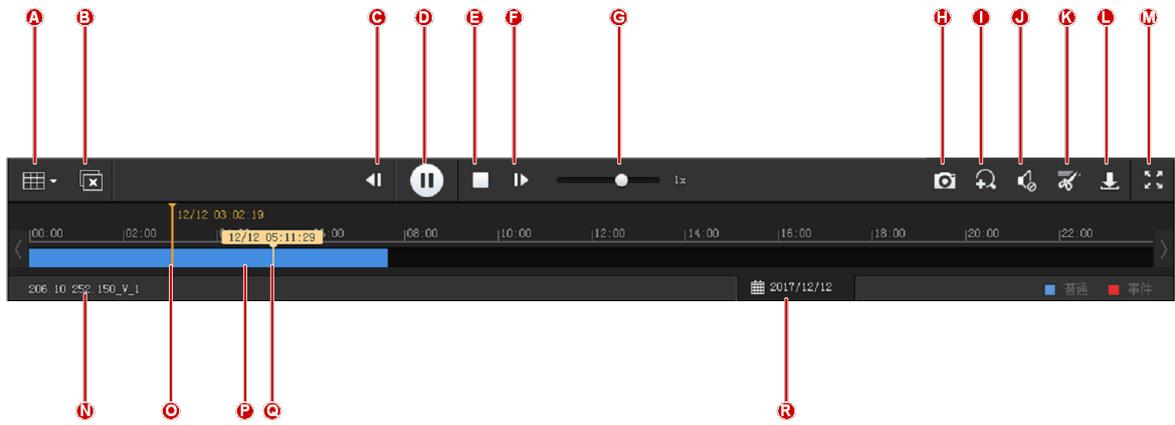
时间轴和文件列表中的查询结果对应当前选中的窗格。单击其他窗格查看对应的查询结果。

回放控制

在右侧文件列表中双击文件或点击播放按钮（）开始播放（鼠标放置在文件上时出现按钮）。



回放过程中使用底部工具栏操作。工具栏上的部分按钮仅对当前选中窗格有效。

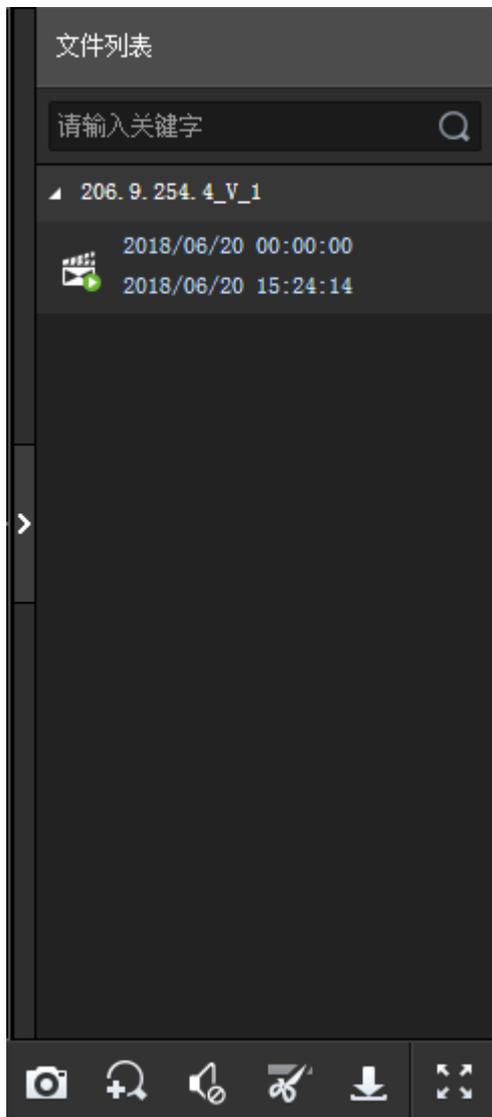


序号	描述
A	切换分屏，最多16分屏。
B	关闭所有窗格的录像。
C/F	单帧后退、单帧前进。
D	暂停/继续
E	停止
G	调整播放速度，有多种倍速可选。+表示正放；-表示倒放。
H	抓取当前视频画面并保存至本地。 保存路径在 本地配置 中设置。
I	数字放大。启用后，按住鼠标左键在画面上拉框，放大指定区域，然后使用鼠标滚轮放大或缩小画面。单击  关闭。
J	调节PC侧的音量输出大小或静音。
K	剪辑要下载的录像片段。点击开始剪辑按钮  ，点击进度条上相应位置，指定录像剪辑的结束位置，然后点击  。
L	录像下载。 可点击页面右上角的  ，查看管理录像下载任务（见 录像下载 ）。
M	全屏、退出全屏。也可以按Esc键退出全屏。
N	摄像机名。
O	播放进度（上方显示对应的日期和时间）。
P	录像轴（蓝色表示普通录像；红色表示事件录像）。
Q	鼠标光标所在位置对应的时间。
R	日历按钮。点击查询当前摄像机其他日期的录像。

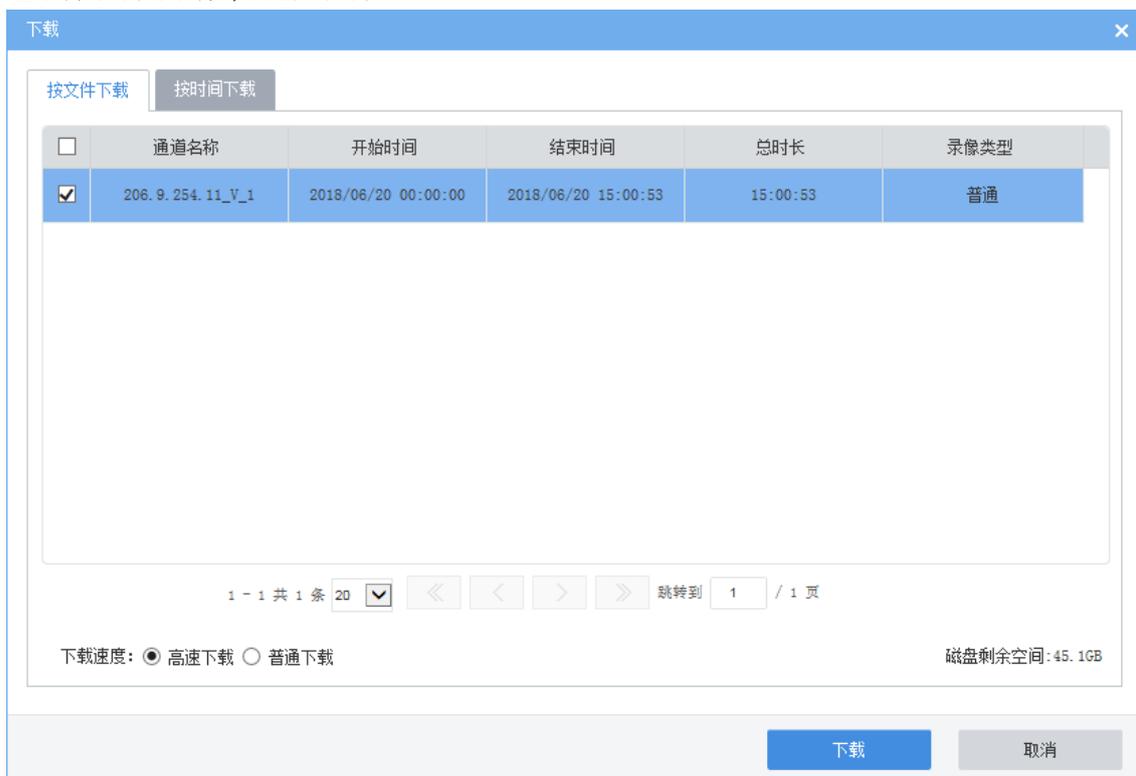
7.3 录像下载

将查询到的录像从平台下载到客户端电脑本地。

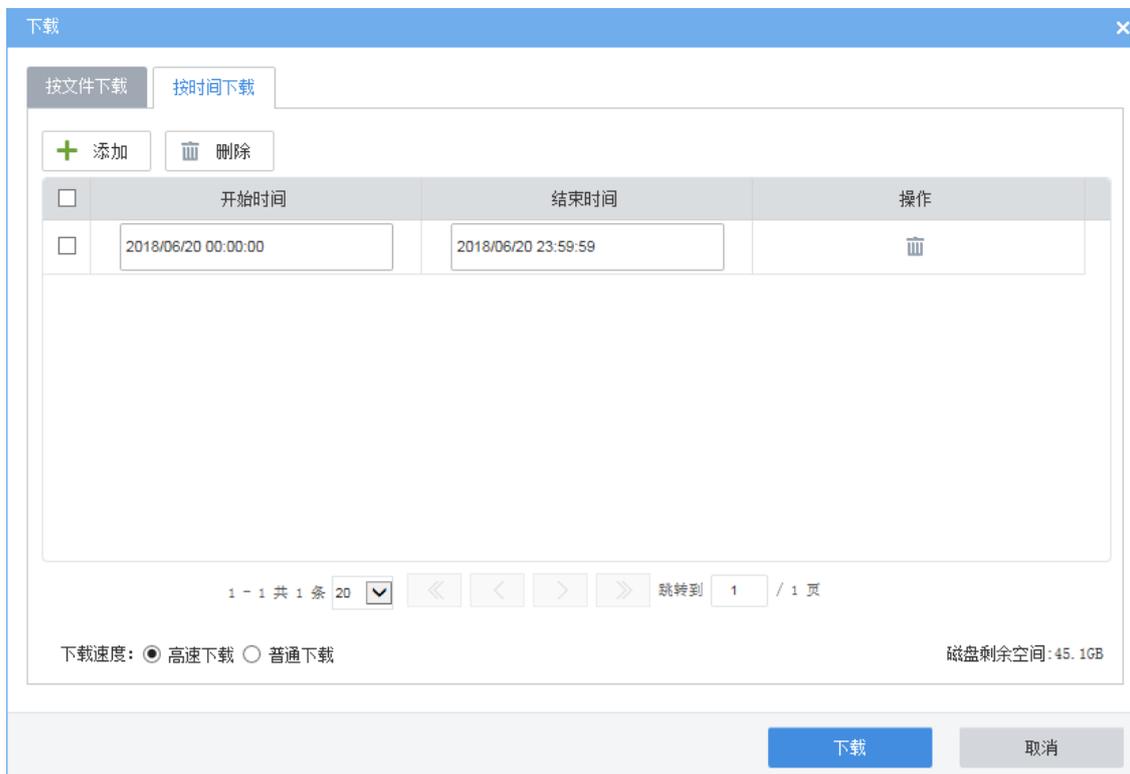
1. 点击工具栏中的 。



2. 选中待下载的录像，点击<下载>。



3. 点击[按时间下载]页签。设置开始和结束时间，下载指定时间段的录像。点击<添加>增加下载任务。完成设置后，选中任务，然后点击<下载>。



说明:

- 下载的录像以“通道名_开始时间_结束时间”的命名格式保存在指定路径，如206.9.9.19_V_1_S20180115000001_E20180115000721.mp4。
- 通道名若包含*或?等特殊字符，特殊字符在录像文件名中显示为下划线。通道名以两个或两个以上空格或点(.)结尾时，最后一个空格或点(.)也显示为下划线。

4. 下载开始后，可点击页面右上角的，查看下载进度、打开下载文件夹、管理下载任务。



7.4 本地配置

视频应用>本地配置

配置视频处理和显示模式、抓图与录像格式及默认保存路径等。

当“媒体流传输策略”设置为“直连优先”时，平台在建立媒体流业务时会根据下行设备的当前剩余发送带宽，选择采用转发或者直连。若直连条件满足，媒体流从下行设备直接发送至客户端，从而节省平台的转发性能消耗；若直连条件不满足，媒体流还是通过平台转发。

当设置为“转发优先”时，媒体流直接通过平台转发。

视频

处理模式	流畅性优先
显示模式	普通品质
媒体流传输协议	TCP
媒体流传输策略	转发优先

图片与录像

抓图格式	<input type="radio"/> BMP <input checked="" type="radio"/> JPEG <input type="radio"/> JPEG & BMP
录像格式	<input checked="" type="radio"/> MP4 <input type="radio"/> TS
文件保存路径	<input type="text"/> <input type="button" value="打开文件夹"/>

说明：本地录像、抓图和下载录像分别保存在该目录的Record、Snap、Download文件夹下。

8 运维统计

运维统计是根据服务器状态、在线用户、存储能力等各类维度进行统计，整体查看当前各类参数状态。通过运维统计可直观了解服务器、设备等数据信息，感知整体态势。还可查询日志，定位异常操作。

支持统计服务器、设备各项指标和查询日志。

8.1 服务器统计

8.1.1 服务器状态

运维统计>服务器统计>服务器状态

查看主从平台服务器的相关信息，包括服务器名称、IP地址、序列号、类型（主机或从机）及状态（在线或离线）。导出信息至CSV文件。可切换至视图模式，查看饼状图。

状态:

名称	IP	序列号	类型	状态
服务器名称	127.0.0.1		主机	<input checked="" type="checkbox"/> 在线

8.1.2 硬盘检测

运维统计>服务器统计>硬盘检测

通过硬盘检测了解硬盘的各类运行指标和状态。可检测扩展柜上的硬盘。

选择盘位和自检类型后点击<开始检测>。检测类型包括：

- 简短型：检测内容少、速度快；
- 扩展型：检测更全面彻底，时间也 longer；
- 传输型：主要检测数据传输时的问题。

自检完成后提示操作成功，并给出整体评估以及自评结果。

盘位选择: 1
 自给类型: 微型型 开始检测 未检测
 生产厂商: WDC
 硬盘型号: WDC [REDACTED]
 硬盘温度 (°C): 26
 使用时间 (天): 639
 整体评估: 健康状况良好
 自评结果: 自我评估未通过时, 继续使用该硬盘。

AttributeID	AttributeName	Status	Hex	CurrentValue	WorstValue	Thresh	ActualValue
200	Multi_Zone_Error_Rate	正常	8	100	253	0	0
199	UDMA_CRC_Error_Count	正常	50	200	200	0	0



说明:

当“整体评估”为除“健康状况良好”之外的其他值时，建议更换硬盘。

8.1.3 网络状态

运维统计>服务器统计>网络状态

选择网卡查看对应的网络配置。如需进行配置，请参考[TCP/IP](#)。

网卡选择: 网卡一

DHCP: 停用

IPv4地址: 192.168.2.27

IPv4子网掩码: 255.255.0.0

IPv4默认网关: 192.168.2.1

网关物理地址: [REDACTED]

MTU: 1500

连接状态: 在线

速率: 100M 全双工

首选DNS服务器: 114.114.114.114

备选DNS服务器: 8.8.8.8

默认路由: 网卡1

8.1.4 在线用户

运维统计>服务器统计>在线用户

查看平台的登录用户信息，包括用户名、登录客户端的IP地址、登录时间和客户端类型（WEB：网页客户端，CS：软件客户端）。

管理员（admin）可以对非管理员用户进行强制下线操作：选中后点击<下线>。被强制下线的用户将退出到未登录状态。

下线 请输入关键字

<input type="checkbox"/>	用户名	登录IP地址	登录时间	登录客户端类型
<input type="checkbox"/>	admin	192.169.1.101	2021/03/23 15:30:48	WEB

8.1.5 带宽统计

运维统计>服务器统计>带宽统计

查看主从平台服务器的实时带宽使用数据。见[网络资源统计](#)。

设备名称	IP	设备类型	IP通道接入	远程回放接入	远程预览	远程回放及下载	网络接收剩余	网络发送剩余
VMS	192.168.4.48	从机	0Kbps	0Kbps	0Kbps	0Kbps	0Kbps	0Kbps
VMS	127.0.0.1	主机	4Mbps	0Kbps	0Kbps	0Kbps	508Mbps	384Mbps

8.1.6 丢包率统计

运维统计>服务器统计>丢包率统计

统计平台通道的收流丢包率。点击<开始统计>和<结束统计>按钮进行操作。

刷新

通道名称	设备名称	所属组织	码流类型	统计结果	操作
192.168.4.234_V_1	192.168.4.234	root	第三流	--	开始统计
192.168.4.239_V_1	192.168.4.239	root	第三流	--	开始统计
192.168.4.239_V_1	192.168.4.239	root	主码流	--	开始统计

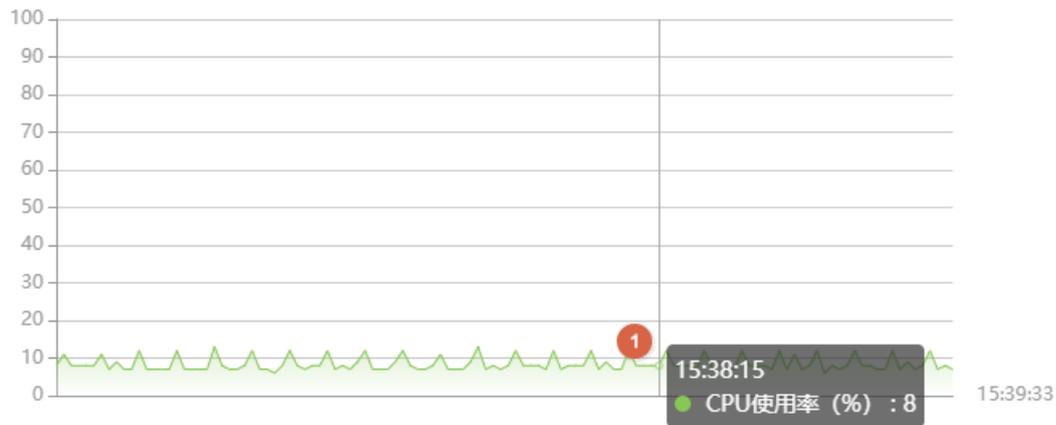
8.1.7 服务器性能

运维统计>服务器统计>服务器性能

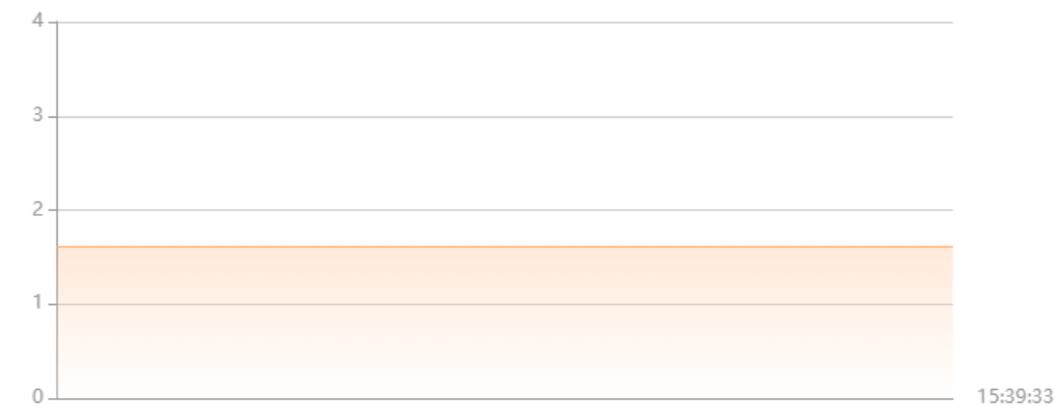
查看平台的CPU使用率、RAM (物理内存) 使用率、发送及接收带宽信息。

打开页面自动开始统计。最多显示240秒的统计结果。可将光标放置在图表上 (如下图1) 查看某一时刻的统计信息。如果配置了多张网卡, 各网卡的统计信息以不同颜色的折线显示。可点击横坐标下的网卡 (如下图2), 选择统计或不统计特定网卡的带宽数据。切换页面会清除统计结果。

CPU使用率 (%)



RAM使用量 (GB)



接收带宽使用情况 (Mbps)



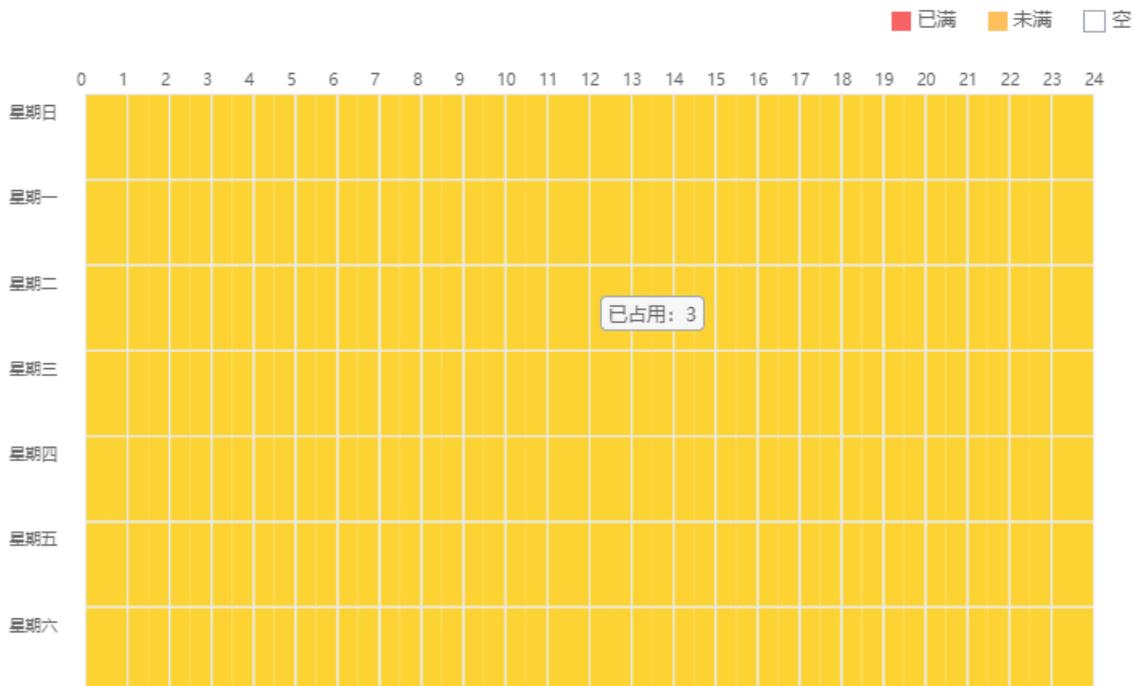
发送带宽使用情况(Mbps)



8.1.8 存储能力

运维统计>服务器统计>存储能力

在配置录像计划（基础配置>录像计划）或备份计划（录像备份>自动备份）时，若系统提示存储能力达到上限，可查看平台的存储能力使用情况，相应修改录像计划或录像备份，释放部分存储能力。



图表中纵轴表示一周各天（周日到周六），横轴表示每天时间（0点到24点，划分成48段）。三种颜色表示三种不同状态。可将鼠标光标放置在图上，查看对应时段占用的存储能力。

- 红色：对应时段无空闲存储能力，不能配置录像计划或自动备份计划。
- 黄色：对应时段有空闲存储能力，可以配置录像计划或自动备份计划。
- 白色：对应时段没有使用任何存储能力，可以配置录像计划或自动备份计划。

若系统提示平台的存储能力已满，可尝试以下操作释放存储能力：

业务类型	尝试操作
录像计划 [基础配置>录像计划]	减少录像计划个数。
录像备份 [录像备份>自动备份]	<ul style="list-style-type: none"> • 减少所选的录像类型。选择的录像类型越多，占用的存储能力越多。 • 改变所选的录像类型。定时录像占用的存储能力大于其他录像类型。 • 修改备份执行时间，比如从每天备份改为一周备份三天。 • 修改录像开始与结束时间，减少不同通道的相同备份时段。 • 降低备份速度。备份速度越高，占用的存储能力越多。



说明：

录像计划和录像备份都占用存储能力。当存储能力达到上限时，可以修改录像计划，将释放的存储能力用来配置录像备份，也可以修改录像备份，将释放的存储能力用来配置录像计划。

8.1.9 录像状态

运维统计>服务器统计>录像状态

按录像状态或录像类型查询录像统计数据。导出查询结果至CSV文件。可切换至视图模式，查看饼状图。将光标放在饼图上可查看百分比。

通道名称	设备名称	所属组织	录像类型	状态	诊断结果	录像容量(GB)	码流类型	帧率(fps)	码率(Kbps)	分辨率
192.168.4.234_V_1	192.168.4.234	根组织	定时录像	开启	正常	6	主码流	15	574	2592x1944(1944P)
192.168.4.239_V_1	192.168.4.239	根组织	定时录像	开启	正常	26	主码流	25	2895	2592x1944(1944P)

8.2 设备统计

设备状态

运维统计>设备统计>设备状态

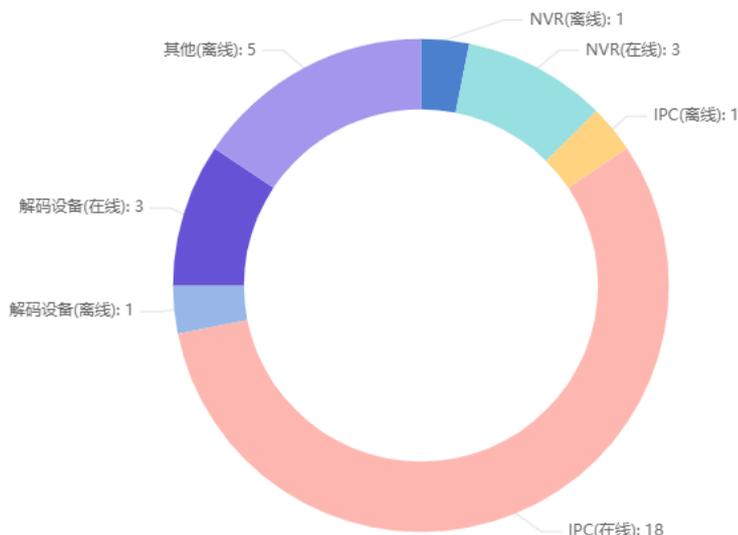
在左侧组织列表中选择需要查看的组织，按设备类型或状态查询设备统计数据。

单击设备列表左侧的 > 查看设备下通道的在线状态。

单击<导出>将查询结果保存至CSV文件。

设备名称	设备类型	组织名称	IP地址	所属服务器	厂家名称	序列号	版本	物理地址	硬盘状态	状态	操作
> 192.168.2.104	NVR	根组织	192.168.2.104		大华				正常	在线	
> 192.168.2.107	NVR	根组织	192.168.2.107		大华				正常	在线	

可切换至视图模式，查看饼状图。将光标放在饼图上可查看百分比。



设备硬盘状态

运维统计>设备统计>设备硬盘状态

在左侧组织列表中选择需要查看的组织，可在右上角输入设备名称进行搜索。

单击设备列表左侧的 > 查看硬盘的在线状态。

单击<导出硬盘信息>将当前页面在线硬盘信息导出至CSV文件。

设备名称	设备类型	所属组织	IP 地址	所属服务器	厂家名称	序列号	版本	物理地址	硬盘状态	在线状态	操作
192.168.2.1 04	NVR	根组织	192.168.2.1 04						正常	在线	

8.3 日志查询

查询、导出平台服务器和设备的报警日志；查询、导出平台服务器的操作日志。

8.3.1 服务器报警日志

运维统计>日志查询>服务器报警日志

查询、确认、导出平台服务器的报警信息。

报警时间段: 2022/10/19 00:00:00 ~ 2022/10/25 23:59:59 当天 最近3天 最近7天 自定义

报警类型: 所有

服务器: 所有

报警确认状态: 所有 报警级别: 1级 x 2级 x 3级 x

查询 重置

报警时间	报警源	报警类型	报警级别	服务器	操作	确认用户	报警确认时间	确认描述	详情
2022/10/20 14:23:27	VMS-@R244	服务器故障	1级						
2022/10/20 14:21:27	HDD2	硬盘上线	5级						
2022/10/20 14:21:27	HDD1	硬盘上线	5级						
2022/10/19 17:15:43	VMS-@R244	服务器故障	1级						

说明:
报警确认后不可撤销。

8.3.2 设备报警日志

运维统计>日志查询>设备报警日志

查询、确认、导出平台下的设备报警信息。

报警源: 所有 请输入关键字

报警时间段: 2024/03/01 00:00:00 ~ 2024/04/02 00:00:00 当天 最近3天 最近7天 自定义

服务器: 所有

报警确认状态: 所有 报警级别: 1级 x +4

查询 重置

报警时间	报警源	报警类型	报警级别	服务器	操作	确认用户	报警确认时间	确认描述	详情
2024/03/29 17:59:41	192.168.1.143_V_1	车辆识别不匹配报警	1级	VMS-@R244					
2024/03/29 17:59:41	192.168.1.124_9_V_1	车辆识别不匹配报警	1级	VMS-@R244					
2024/03/29 17:59:41	192.168.1.127_V	车辆识别不匹配报警	5级	VMS-@R244					

说明:

- 报警源选择“所有”时，支持输入报警源名称关键字进行模糊查询；报警源选择具体类型时，可选择具体报警源和报警类型。
- 报警确认后不可撤销。

8.3.3 操作日志

运维统计>日志查询>操作日志

查询、导出用户操作信息。

操作用户:	<input type="text"/>		
日志业务类型:	所有	日志操作类型:	所有
操作时段:	当天	<input type="text" value="2020/11/19 00:00:00"/>	<input type="text" value="2020/11/19 23:59:59"/>

导出	重置	查询						
时间	操作用户	IP地址	主类型	子类型	操作对象	所属设备	所属组织	操作结果
2020/11/19 10:23:54	admin	192.169.1.101	登录	用户登录	admin	-	-	成功

说明:
 实况上墙、回放上墙的操作对象格式如下：电视墙名称/窗口索引/分屏索引。若后跟“-”，则默认情况下表示编码通道/码流。举例：-203.130.1.35-1/0，则“203.130.1.35-1”指IP地址为203.130.1.35的编码设备的1号编码通道；0表示主流（1：辅流，2：三流）。

9 门禁管理

门禁控制是对添加到平台的门禁设备进行统一管理，给人员分配通行权限、门卡和房屋，用于控制人员出入和人员相关信息。安装考勤组件后还支持对人员考勤进行管理，可满足企业、园区等考勤需求。通过设置考勤时段、考勤班次等信息后，人员可通过在门禁设备上刷脸、刷卡或人证核验等方式进行考勤签到。

说明:
 20A16-DT型号的服务器不支持**管理考勤**。

通过门禁控制可配置门组和时间模板，分配人员进出门禁的权限，分配及绑定人员门卡和房屋所属关系，实现对人员的管理。例如，物业为小区内住户开通访问小区各出入口门禁权限并根据所在房屋分配单元楼门卡，人员可在小区内自由进出，方便管理。可广泛应用于社区、企业、园区等场所。

支持管理门禁权限、门卡和房屋。

9.1 权限管理

门禁管理>权限管理

管理时间模板、门组和门禁授权。

9.1.1 时间模板

通过时间模板限制门禁权限的生效时间。创建好的时间模板在**门禁授权**中使用。

系统自带All-day模板，可以编辑，但不能删除。分配All-day模板表示没有门禁时间限制。

具体配置操作与**用户时间模板**类似。

9.1.2 门组

门组即一组门的集合。创建门组便于门禁授权。需要先在[基础配置>设备管理]下完成添加门通道。具体请见**门禁设备**和**门禁通道**。

新增

名称: 复制模板

未选设备	已选设备
<input type="text" value="请输入关键字"/> <input type="button" value="Q"/>	<input type="text" value="请输入关键字"/> <input type="button" value="Q"/>
<input checked="" type="checkbox"/> 根组织 <input checked="" type="checkbox"/> 192.168.2.13 <input checked="" type="checkbox"/> 192.168.2.33	<input type="checkbox"/> 根组织
<input type="button" value="»"/> <input type="button" value="«"/>	

备注:



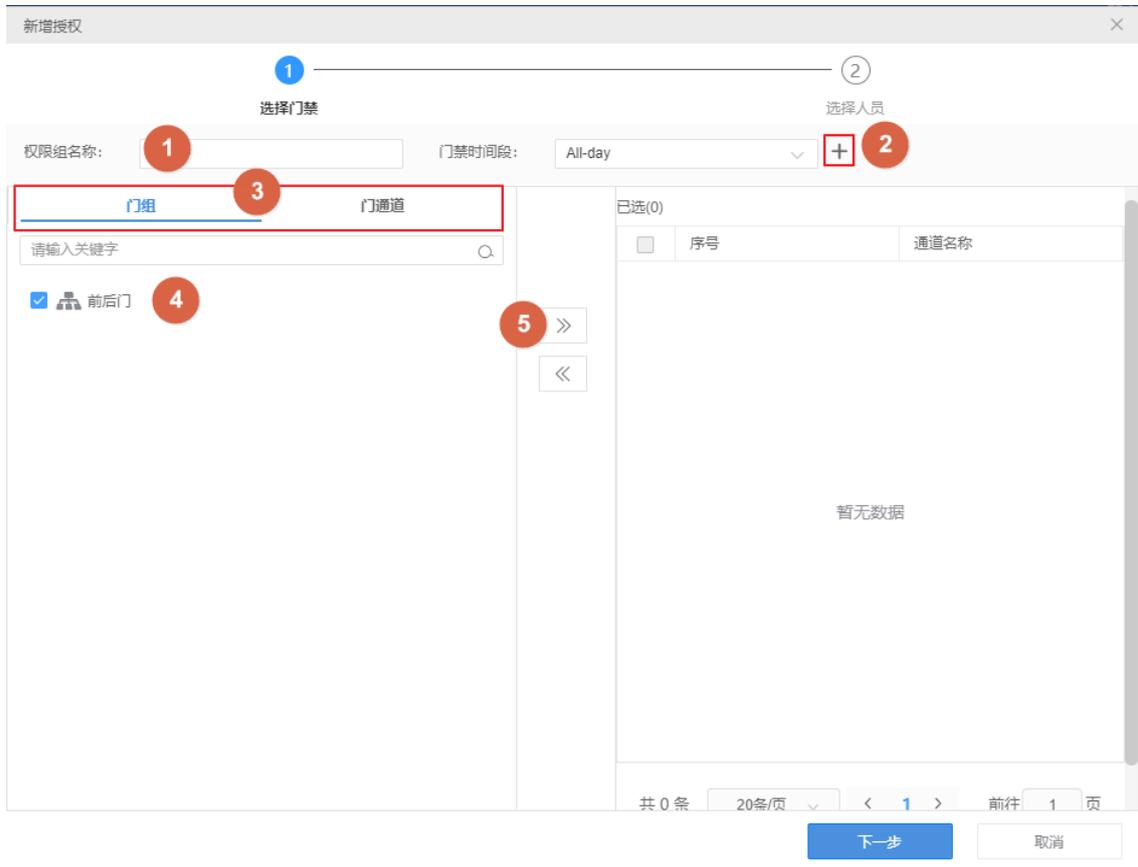
说明:

可勾选“复制模板”，复制已有门组的配置。

9.1.3 门禁授权

向指定人员分配指定门组或门的权限。

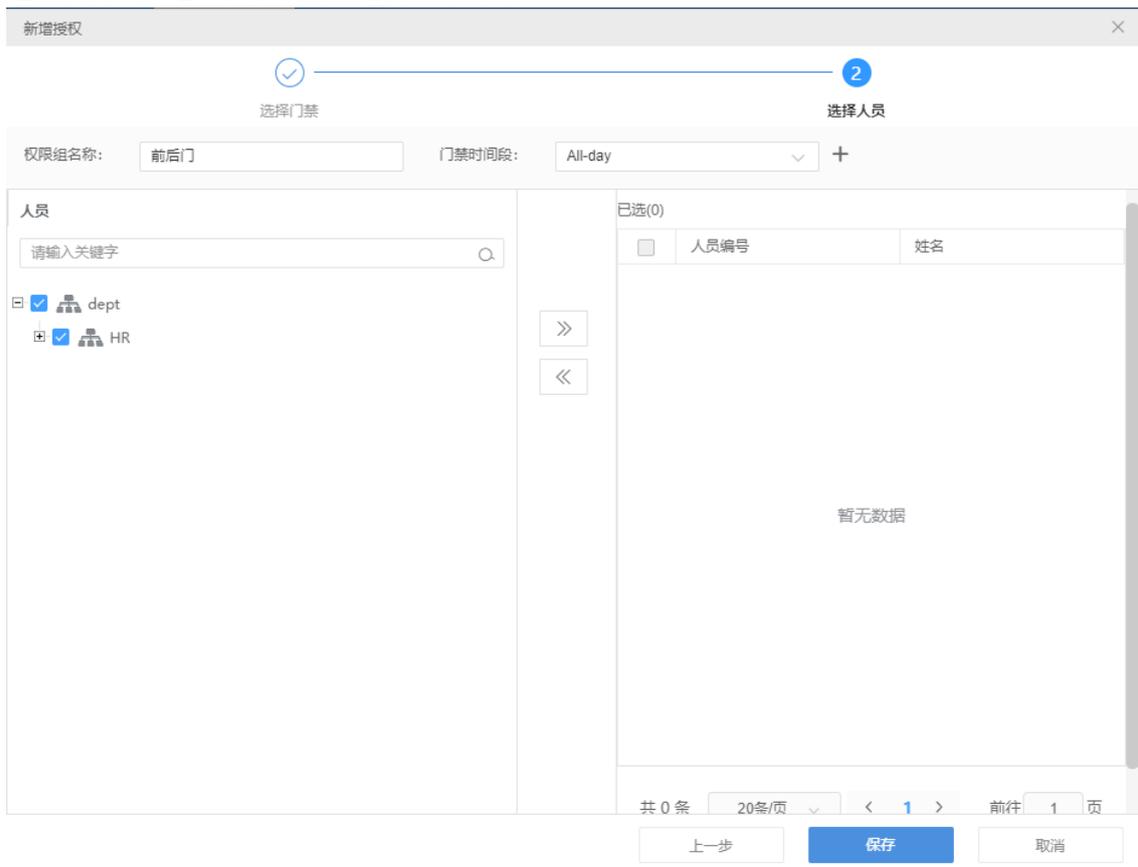
1. 单击[新增授权]。
2. 选择门禁。



说明:

- 步骤2：可选择已有时间模板或新建时间模板。时间模板用于限制门禁时间段。
- 步骤3：可点击[门组]或[门通道]页签，选择门组或门（门通道）。

3. 选择人员。所选人员被授权指定门禁的权限。



4. 点击<保存>。
5. 点击[操作]列中的  查看授权是否成功。

9.1.4 核验模板

核验模板用于设置门禁在不同时段的核验方式，可在配置门禁通道时直接关联核验模板，应用预设配置。



该截图展示了“门卡管理”下的“核验模板”配置界面。界面顶部有“权限管理”和“门卡管理”标签。左侧是模板列表，包含“default”和“hhh”。主区域显示了模板名称“核验”（标注2），以及按星期一至星期日的时段配置表。配置表包含“时间段1”至“时间段8”，每个时段可设置开始/结束时间（标注3）和核验方式（标注4）。核验方式列表包括：人证核验、人脸白名单、人证+号码白名单、号码白名单、人脸白名单、密码比对、人证+号码白名单、号码白名单+人脸白名单、人证+刷卡、指纹白名单。底部有“复制到”选项（标注5）和“确定”、“取消”按钮。

1. 单击+新增核验模板，或者选择已有的核验模板进行修改。
2. 设置模板名称。
3. 选择每日的核验时间段和核验方式。
4. 设置好某一天后，可选择其他日期，单击<复制>，快速应用当前日期的核验模式到其他日期。
5. 单击<确定>保存。

9.2 门卡管理

门禁管理>门卡管理

查看不同状态的卡，进行挂失、解挂等操作。

激活卡

门禁管理>门卡管理>激活卡

激活卡指当前可以正常使用的卡。开卡后卡片处于激活状态。可修改激活卡的有效期或进行挂失。

挂失 请输入关键字

<input type="checkbox"/>	序号	卡号	卡状态	姓名	性别	人员编号	部门	联系电话	操作
<input type="checkbox"/>	1	100200	激活	张三	男	001	HR		

冻结卡

门禁管理>门卡管理>冻结卡

挂失的卡处于冻结状态，不可使用。可以对挂失卡进行解挂。解挂后卡片处于激活状态，可正常使用。

可以对挂失卡进行补卡操作，即重新开一张卡替代挂失卡。补卡后，挂失卡变为注销卡。

解挂 请输入关键字

<input type="checkbox"/>	序号	卡号	卡状态	姓名	性别	人员编号	部门	联系电话	操作
<input type="checkbox"/>	1	1237	冻结	002	男	002	新节点1		

空白卡

门禁管理>门卡管理>空白卡

空白卡指未分配的卡。点击<新增>或<导入>添加空白卡。

+ 新增		删除	导入	请输入关键字	
序号	卡号	卡片类型	卡状态	操作	
1	100202	IC卡	空白	🗑	
2	100205	IC卡	空白	🗑	

注销卡

门禁管理>门卡管理>注销卡

对挂失卡进行补卡操作后，挂失卡处于注销状态。注销的卡不能再使用。

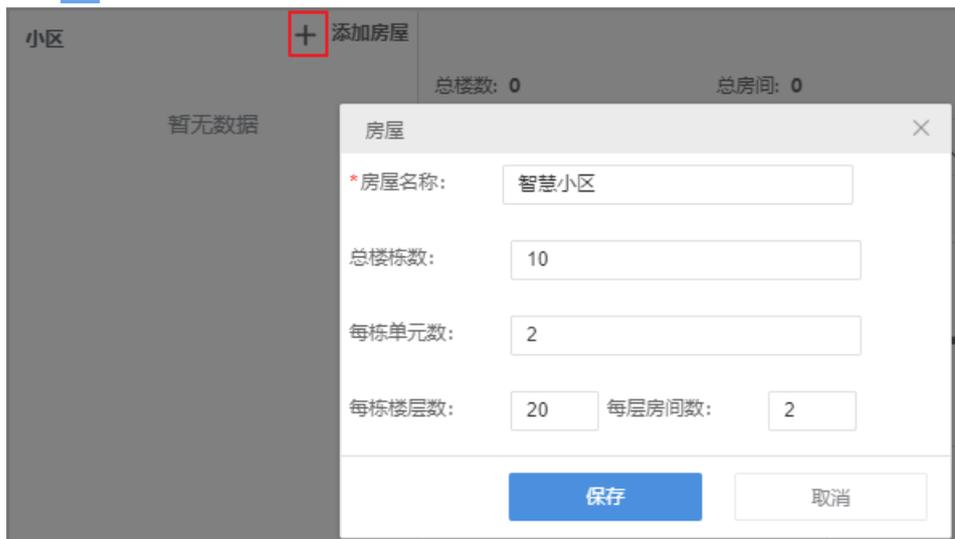
序号	卡号	卡状态
1	100203	注销

9.3 小区管理

管理小区、宿舍等房屋资源以及人员入住情况。

9.3.1 添加房屋

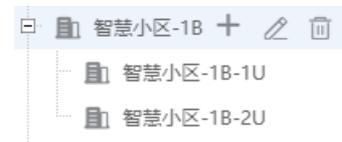
1. 单击 **+** 添加房屋，根据界面提示完成设置。



2. 添加完成后，房屋信息、总楼数、房间数等信息显示在页面顶部。



3. 根据需要修改名称，添加或删除楼栋、单元等。



4. 点击单元，在房间列表中查看该单元的房间。可修改房间名称或删除房间、添加房间。



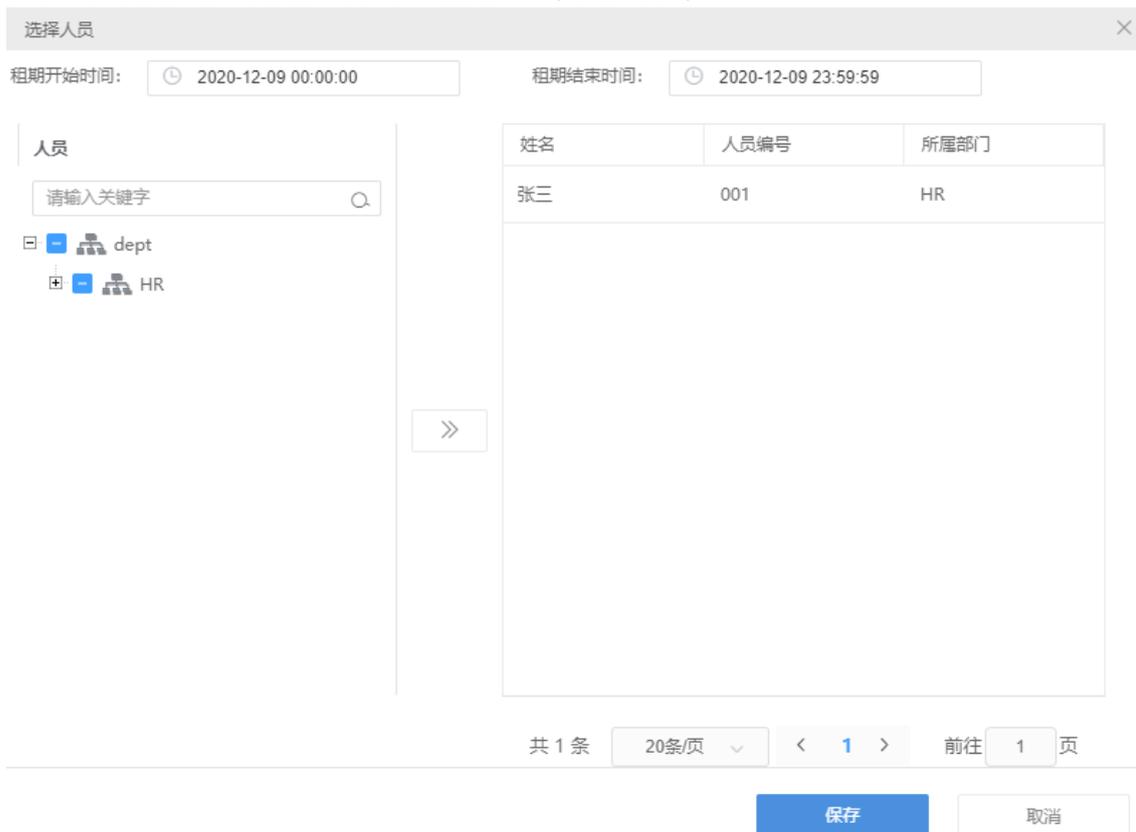
9.3.2 入住人员管理

房间列表中，红色表示有人入住，绿色表示无人入住。可增加或删除指定房间的入住人员。

1. 选定房间，单击+号添加入住人员。



2. 从左侧列表中选择人员进行添加。列表中的人员在[基础配置>人员管理]中添加（见[人员管理](#)）。设置租期。租期满后，该房间在列表中显示为橙色（表示到期）。



3. 人员添加完成后，房间变为红色，表示有人入住，同时显示入住人员以及租期结束时间。根据需要，重复上述步骤继续添加人员。



4. 若要将入住人员从房间中清除，先勾选人员，然后点击<退租>；或者点击人员右上角的<编辑>按钮，修改房间和租期。

9.4 考勤管理

设置考勤制度、人员排班，进行考勤处理及统计操作。(VMS-20A16-DT不支持该功能。)

说明:

- 使用考勤管理前需安装**考勤组件**。
- 考勤计算精度均精确到分，考勤计算、打卡时间均只取分钟数，忽略秒数。即08:00:59打卡视作08:00。

9.4.1 考勤制度

设置考勤规则。

设置考勤自动计算时间，系统每天将会在所设时间计算前一天的考勤数据，可在考勤明细中查看。若某天自动计算考勤时未成功，可参见**考勤明细**手动进行计算。

考勤规则

* 考勤自动计算时间:

05:00



保存

9.4.2 人员排班

9.4.2.1 时间段设置

选择时间段类型并进行相应设置，时间段类型可设置为普通时间段和弹性时间段。

- 普通时间段：正常上下班，员工必须在规定的有效签到/签退时间段中打卡上下班。
- 弹性时间段：弹性工作制，员工可在任意时间上下班，通过设置的弹性时长计算方式计算每日出勤时长。

普通时间段

Q 请输入关键字

(普通) 早班

(弹性) 中班

* 时间段名称: 早班

* 时间段类型: 普通时间段

时间段设置

* 上班时间: 09:00 * 有效签到时间: 08:30 ~ 09:30 必须签到

* 下班时间: 18:00 * 有效签退时间: 17:30 ~ 18:30 必须签退

缺勤设置

已签到, 迟到超过 0 分钟, 记为迟到

已签退, 早退超过 0 分钟, 记为早退

未签到, 记为 缺勤

未签退, 记为 缺勤

保存

1. 单击.
2. 输入时间段名称。
3. 选择时间段类型为：普通时间段。
4. 选择上下班时间。当下班时间早于上班时，自动+1天。上/下班时间需在有效签到/签退时间范围内。
5. 设置人员是否必须签到/签退。
 - 必须签到/签退。
 - (1) 选择有效签到/签退时间：设置上下班的有效打卡时间段，包括边界值。即设置有效签退时间为17:30-18:30，则可签退时间即为17:30-18:30。
 - (2) 配置缺勤设置。
 - 已签到，迟到超过x分钟，记为迟到：晚于上班时间x分钟之内，考勤状态为正常，x不超过999。
 - 已签退，早退超过x分钟，记为早退：早于下班时间x分钟之内，考勤状态为正常，x不超过999。
 - 不必签到/签退，去除勾选。
6. 单击<保存>。



说明:

- 当时间项出现+1标志时，即代表跨天。请注意跨天的所有时间项均不可晚于考勤自动计算时间。
- 有效签到时间范围与有效签退时间范围不可重叠。

弹性时间段

+

🗑️

🔍 请输入关键字

🕒 (普通) 早班

🕒 (弹性) 中班

* 时间段名称:

* 时间段类型:

* 弹性时长计算方...

* 有效打卡间隔时长: 分钟

时间段设置

* 每日工作时间: 分钟

* 跨天打卡时间切... 🕒

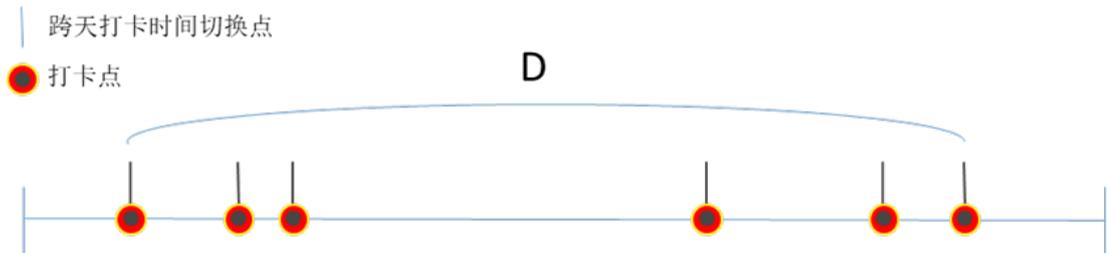
1. 单击+

2. 输入时间段名称。

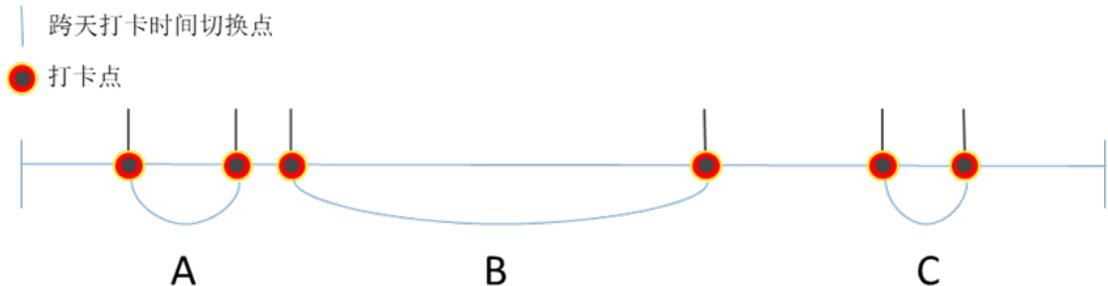
3. 选择时间段类型为：弹性时间段。

4. 选择弹性时长计算方式。

- 首尾打卡计算时长：取考勤日中最早打卡时间作为上班时间，最晚打卡时间作为下班时间，计算出勤时长。即出勤时长为下图中D时间段时长。



- 两两打卡累计时长：取考勤日中每两条打卡时间差，累计计算当日出勤时长。即出勤时长为下图中A+B+C时间段总时长。若当日打卡次数为奇数，管理员可根据实际情况补签后再计算人员考勤，否则当日打卡均视为无效。



5. 设置有效打卡间隔时长。打卡与前一次有效打卡间隔时间需大于等于所设定时长才认定为有效，避免误刷卡。



说明:

仅弹性时长计算方式选择两两打卡累计时长时，才显示该配置项。

6. 设置每日工作时间。若出勤时长少于每日工作时间将记为缺勤。

7. 设置跨天打卡时间切换点，在该时间点切换为下一个考勤日。例如：设定01:00为跨天打卡时间切换点，则考勤日为当日01:00至次日00:59，员工在次日00:59（包含）前打卡视为今日考勤打卡，在次日01:00（包含）后打卡视为次日考勤打卡。

8. 单击<保存>。

更多操作

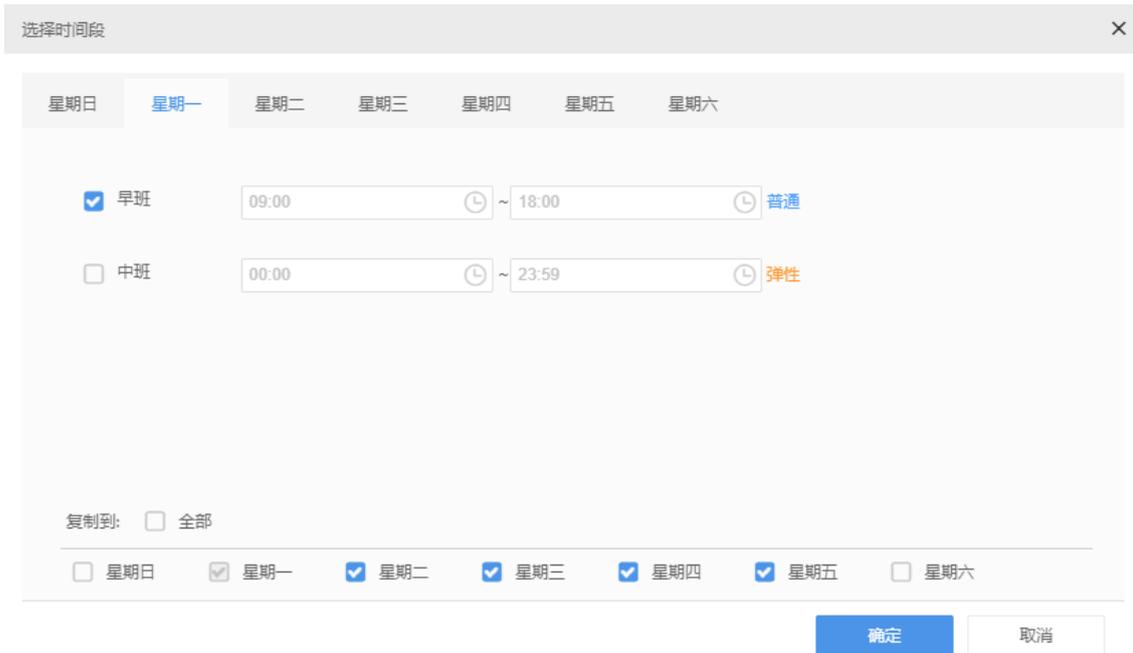
支持对时间段进行修改、删除操作。

- 修改时间段信息：单击时间段名称，即可在右侧窗口中修改对应信息。
- 删除时间段：选择需要删除的时间段，单击上方的 ，确认后即可删除。

9.4.2.2 班次管理

设置班次并选择对应工作时段。

1. 单击 ，输入班次名称新增班次并设置班次周期。
2. 单击<选择时间段>。



3. 选择班次开始的工作日。
4. 勾选在[时间段设置](#)中设置的时间段，为该时间段设置班次。
5. 选择该时间段对应的工作日。可勾选<全部>一键复制到周一到周日。
6. 单击<确定>。

单击<清空>可以清空所有有效时间段。



说明:

单个班次最多可设置8个时间段。

更多操作

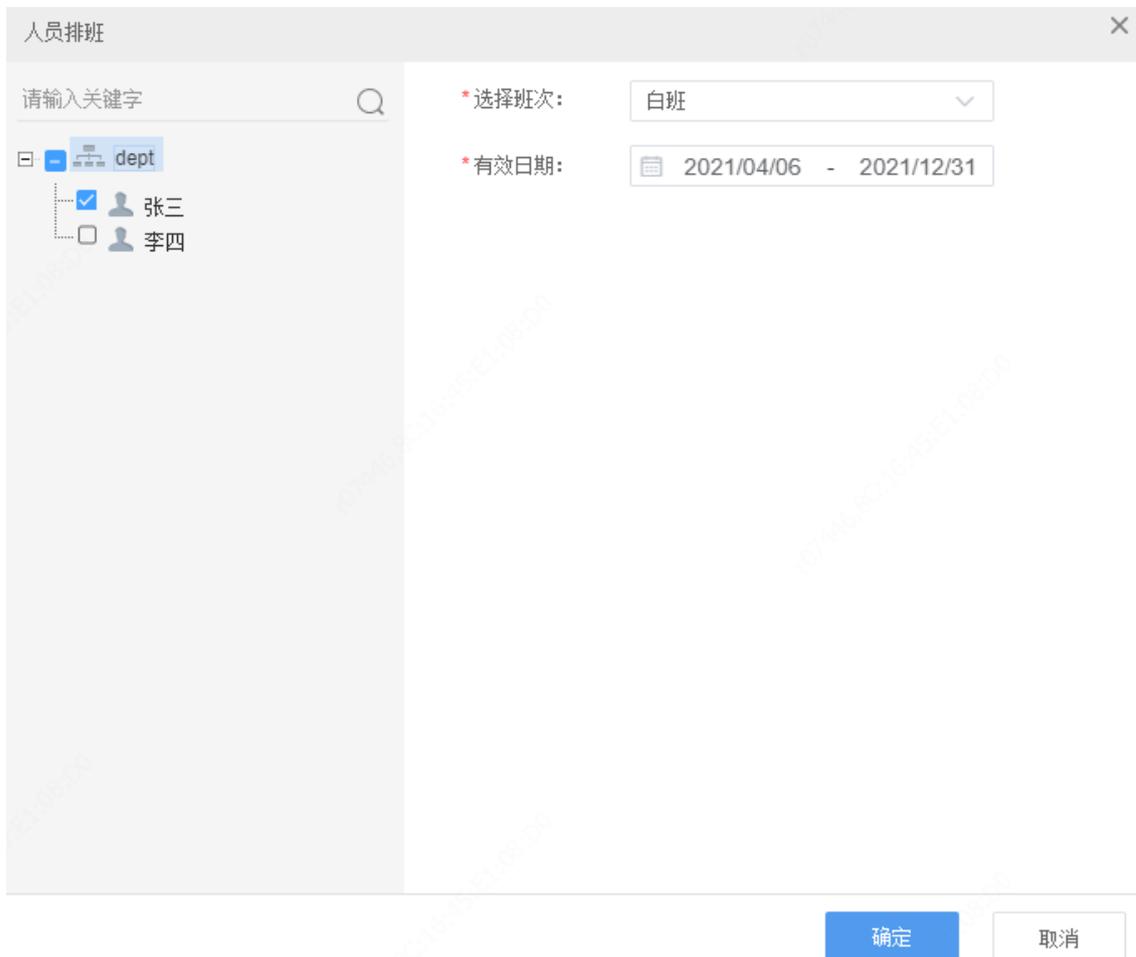
支持对班次进行修改、删除操作。

- 修改班次信息：单击班次名称，即可在右侧窗口中修改对应信息。
- 删除班次：选择需要删除的班次，单击上方的 ，确认后即可删除。

9.4.2.3 排班管理

为部门或人员设置班次。

1. 单击<人员排班>。



2. 勾选需要排班的部门或人员。
3. 选择班次并设置有效日期。
4. 单击<确定>。

 **说明:**

- 可通过设置不同有效期的排班为人员在不同时间段内安排班次。
- 人员每日仅允许存在一个排班。若新旧排班有效期有重叠，则重叠部分日期安排新排班。

勾选排班记录单击上方的<取消排班>取消排班。

9.4.3 考勤处理

9.4.3.1 请假处理

添加

*请假人员: 李四

*请假主类型: 请假

子类型: 事假

*请假开始时间: 2022/06/27 09:00

*请假结束时间: 2022/06/27 18:00

时长(分钟): 540

备注:

提示: 请假/补签操作不会自动计算考勤, 请到“考勤明细”界面进行手动计算

确定 取消

1. 在组织列表中选择需要请假的人员。
2. 单击[请假/出差]。
3. 在弹出的[添加]框中输入请假主类型，请假开始、结束时间等。
4. 选择子类型。



说明:

仅当请假主类型选择<请假>时，显示子类型选择框。

5. 单击<确定>。

更多操作

支持对请假/出差记录进行修改、删除操作。

- 修改：单击操作栏下的 修改人员请假类型、时间等。
- 删除：单击操作栏下的 删除请假。

9.4.3.2 补签处理

当人员考勤状态异常时（比如缺勤、迟到等），支持手动更正签到或签退记录。补签后，用户可在[考勤明细](#)中单击<考勤计算>来更新对应日期的考勤状态及缺勤时长。

起止时间	工作日	部门	人员编号	姓名	班次名称	上下班时间段	签到时间	签退时间	考勤状态	缺勤时长	操作
2021-02-26		dept	11	11	1	02:00-08:00	(-)	(-)	缺勤	6小时	

1. 在左侧组织列表中，选择部门或选择人员。
2. 选择起止时间，显示所选部门或人员在该时间段内的考勤异常。
3. 单击需要处理考勤异常人员操作列下的 （补签到）或 （补签退）。
4. 根据实际情况选择补签时间。

5. 单击<确定>。

说明:

- 补签时间需在签到开始时间到签退结束时间内，否则补签无效。
- 单人单日补签条数上限为100条，超过100条时需手动清理该人员当日的补签记录，才能继续补签。
- 若多次补签，系统会使用有效时间范围内最早和最晚的时间作为补签时间。

9.4.3.3 补签记录

手动更正签到或签退时间后将生成补签记录，在此界面可以查询、编辑或删除补签记录。

1. 在左侧组织列表中，选择部门或选择人员。
2. 选择起止时间、处理类型，单击<查询>显示所选部门或人员在该时间段内的补签记录。

人员编号	姓名	部门	处理类型	补签时间	操作时间	操作
11	11	dept	补签	2021/02/26 08:00	2021/02/27 10:00	编辑 删除

更多操作

支持对补签记录进行修改、删除操作。

- 单击 可修改补签时间。
- 单击 可删除补签到/补签退记录，删除后考勤统计中将使用该人员当天对应签到/签退时间段的原始考勤数据。

9.4.4 考勤统计

考勤统计中仅统计已添加至该系统的人员考勤，陌生人员进出仅在过人记录中显示，不计入考勤。

原始数据：查看起止时间段内人员通过刷脸或刷卡出入的所有记录。

考勤明细：查看起止时间段内考勤明细，显示考勤状态、缺勤时长等信息。每人每日仅一条记录。

考勤汇总：查看人员在起止时间段内累计考勤缺勤时长和明细。

9.4.4.1 原始数据

查看起止时间段内人员通过刷脸或刷卡出入的所有记录。例如，当日出入门禁共五次，即显示五条记录。

通过设置过滤条件，可搜索查看某部门或人员的信息记录，包括人员编号、姓名、部门、设备名称、时间、体温、是否佩戴口罩。

人员编号	姓名	部门	设备名称	时间	体温(°C)	口罩
1	1	dept	206.10.81.13	2022-06-27 11:46	36.5°C	否

1. 在组织列表中选择部门或人员。
2. 设置考勤起止时间。
3. (可选) 设置体温范围、是否戴口罩。需要门禁设备支持并配置对应功能。
4. 单击<查询>。

搜索到的人员出现在列表中，可单击<导出>，导出人员数据。

9.4.4.2 考勤明细

查看起止时间段内考勤明细，显示考勤状态、缺勤时长等信息。每人每日仅一条记录。当天的所有原始数据都将在第二天的考勤自动计算时间进行处理并生成考勤明细。

若某天自动计算考勤时未成功或有人员班次变动，可在左侧组织列表中选择部门或人员并设置起止时间，单击<考勤计算>重新计算所选人员的考勤并生成考勤明细。



说明:

若计算某日考勤时存在班次异常、班次尚未开始/结束的人员，则这部分人员的当日已有考勤将被删除。

通过设置过滤条件，可搜索查看某部门或人员的信息记录，包括人员编号、姓名、部门、日期、时间、签到/签退时间等。

工作日	部门	人员编号	姓名	班次名称	上下班时间段	签到时间	签退时间	出勤时长(分)		考勤状态	缺勤时长(分)	备注
								实际	有效			
2022-06-13	dept	x01234	张三	Default Shift	09:00-18:00	(~)	(~)	0	0	缺勤	540	

搜索到的考勤数据出现在列表中，可单击<导出>，导出人员考勤明细。

9.4.4.3 考勤汇总

查看人员在起止时间段内累计考勤缺勤时长和明细。例如，每月汇总计算出人员当月累计迟到、早退、缺勤等时长。

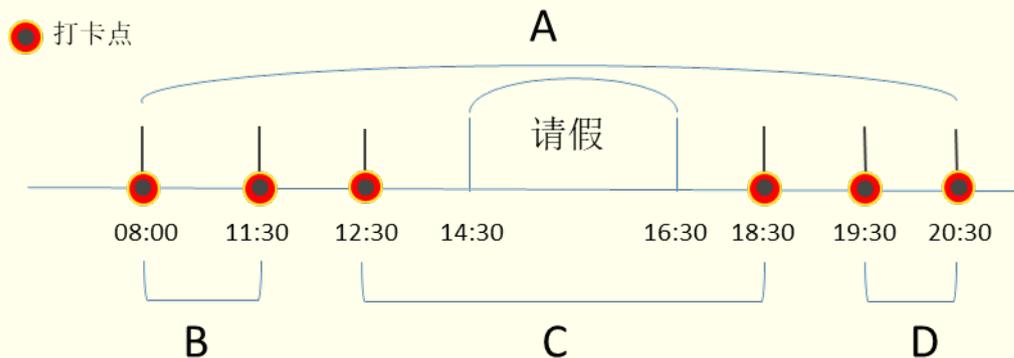
通过设置过滤条件，可搜索查看某部门或人员的信息记录，包括人员编号、姓名、部门、考勤异常、考勤明细等。

部门	人员编号	姓名	迟到时长	早退时长	缺勤时长	请假时长	考勤明细
人力资源部	002	张三	30分钟	30分钟	6.00小时	0分钟	



说明:

弹性时间段的出勤时长和缺勤时长均不会扣除该时间段内的请假时间。即人员考勤计算方式为首尾打卡计算时长时，出勤时长为A时间段时长；考勤计算方式为两两打卡累计时长时，出勤时长为B+C+D时间段总时长。缺勤时长为每日工作时间-出勤时长。



搜索到的考勤数据出现在列表中，可单击<导出>，导出人员考勤汇总数据。

单击考勤明细列下方的查看该人员考勤明细。

工作日	部门	人员编号	姓名	班次名称	上下班时间段	签到时间	签退时间	考勤状态	缺勤时长	备注
2021/04/05	dept	001	张三	白班	14:00-22:00	2021/04/05 14:00	2021/04/05 22:00	正常	0分钟	

10 平台直连公网的端口映射配置指导

平台支持接入宇视云，支持添加云端IPC/NVR，以及通过客户端和EZView远程访问。为保证体验，应优先保证平台直连公网（即具备公网IP或者能够通过单层端口映射连接到公网）。

此指导介绍平台直连公网的端口映射配置相关操作。

10.1 准备

在开始具体配置前，先判断当前平台和互联网间是否只有一次网络地址转换（下文简称NAT）。

1. 查看平台所连接的路由器WAN口IP。
2. 在百度搜索“IP”，查看当前网络的公网出口。
3. 若两者一致，则说明当前为单层NAT。在此基础上继续进行下面的配置步骤。

10.2 路由器配置

市场上在售的大部分路由器均支持端口映射（或叫UPnP或虚拟服务器，不同厂家或级别的路由器在称呼上可能有所差异）。以下举例对两种配置进行介绍。

UPnP

不同品牌路由器的配置入口可能不同，可以自行搜索配置入口。

1. 登录路由器配置界面后，找到UPnP的设置页面。
2. 点击“系统设置”。



3. 点击“高级功能”。



4. 点击高级功能菜单下“UPnP”。



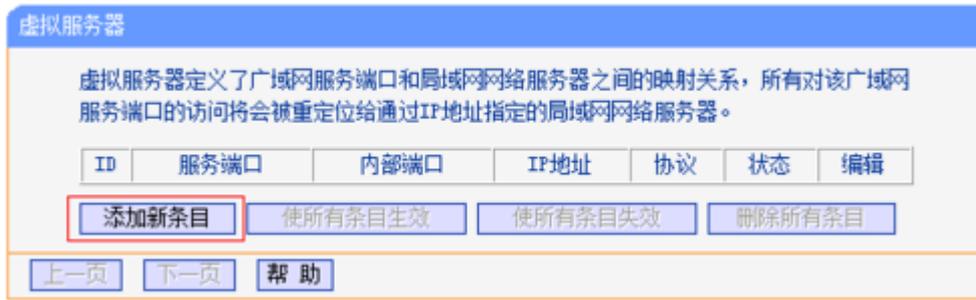
5. 可以看到“UPnP状态”按钮，将其打开为ON。



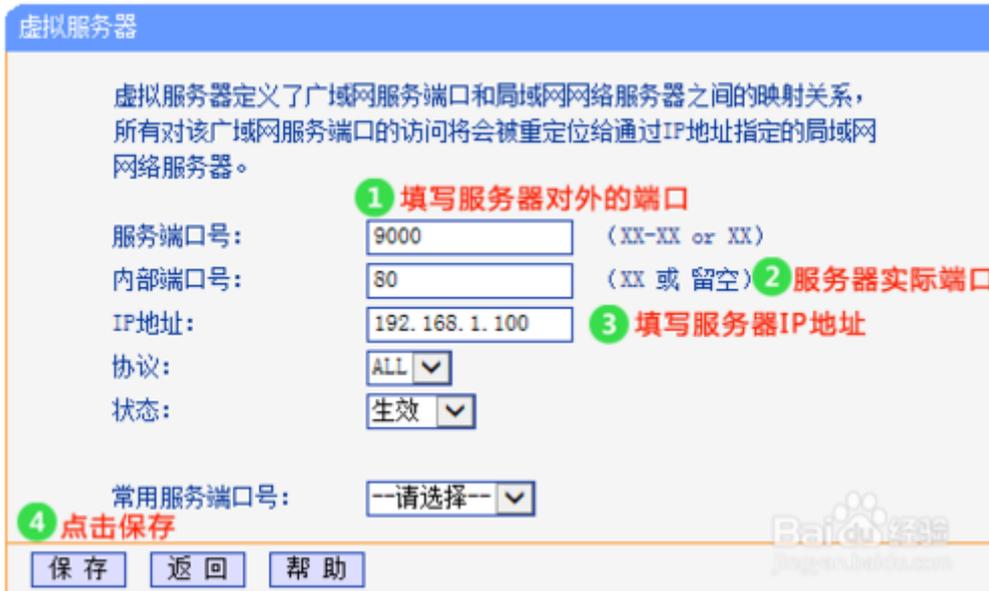
虚拟服务器

不同品牌路由器的配置入口可能不同，可以自行搜索配置入口。

1. 登录路由器管理界面，进入 转发规则 > 虚拟服务器。
2. 添加新条目。



3. 添加服务器映射到外网的端口、实际端口、以及服务器IP地址。



说明:

一些低端路由器不支持配置服务端口号，只支持将内部端口号一一映射为相同的服务端口号。对于这类路由器，在配置端口映射时需修改设备的内部HTTP端口为非80（因为有相关文件要求公网IP的80端口未报备不允许开放）；修改后，无论从外部还是从内部访问设备时，都使用新配置的端口号，例如，61.164.52.152:88对应192.168.1.112:88，内外HTTP端口一致且不为80。

10.3 平台配置

在平台的Web客户端上完成以下配置。

配置DNS服务器地址

1. 系统配置 > 网络配置 > TCP/IP。
2. 手动填写时，DNS服务器地址国内一般使用114.114.114.114或路由器地址。

配置端口映射

1. 系统配置 > 网络配置 > 端口映射。
2. 开启端口映射。
3. 映射方式：若路由器使用UPnP，则映射方式为UPnP；若为虚拟服务器，则映射方式为手动。

端口映射 开启 关闭

映射方式

UPnP映射类型

端口类型	外部端口	外部IP地址	内部端口	设备IP	状态
HTTP端口	50080	N/A	80	192.168.1.60	未生效
RTSP端口	50554	N/A	554	192.168.1.60	未生效
HTTPS端口	50443	N/A	443	192.168.1.60	未生效
报警端口	52080	N/A	52000	192.168.1.60	未生效
SIP端口	55063	N/A	5063	192.168.1.60	未生效

- UPnP自动协商：端口映射的端口由路由器和设备协商分配，随机生成。
 - UPnP指定端口：端口映射的端口由用户指定。注意指定的端口要保证可用，否则映射关系不生效。
 - 手动映射：同样注意填写的端口真实可用。
4. 配置完成后，检查所有端口映射生效。此时设备直连接入公网，同时也可访问EZCloud。在EZCloud的Web界面上显示设备状态为“在线”，即说明当前设备已是直连方式接入公网。

配置成功样例

平台

TCP/IP 子网云 DNS 端口 端口映射 邮件 国际服务器设置 国际本地设置

UPnP 开启 关闭

映射方式

端口类型	外部端口	外部IP地址	内部端口	设备IP	状态
HTTP端口	59270	206.10.12.112	80	100.100.100.101	生效
RTSP端口	50292	206.10.12.112	554	100.100.100.101	生效
HTTPS端口	51838	206.10.12.112	443	100.100.100.101	生效

EZCloud

我的云端设备

选择	序号	组织	设备名称	设备类型	设备IP	最近上线时间	设备状态	共享设备	修改设备	忘记密码	设备访问
<input type="checkbox"/>	1	root	VMS	VMS-摄像头	206.10.12.112	2017/8/26 16:03:05	在线	共享	修改	找回	访问

配置完成后可以使用“telnet 外部IP 外部port”的方式检验是否真实生效。

```

C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation. 保留所有权利。

C:\Users\c02448>telnet 206.10.12.112 50092
  
```

后续说明

若平台无法满足上述直连公网的条件，也应尽量避免以下NAT类型组合：

- 客户端侧为端口受限型NAT，设备侧为对称型NAT；
- 客户端侧为对称型NAT，设备侧为端口受限型NAT；
- 客户端和设备侧均为对称型NAT；

可在宇视云页面下，点击[设备网络类型检测]旁的<检测>按钮，查看当前平台设备侧的网络信息。

宇视云	<input checked="" type="radio"/> 开启 <input type="radio"/> 关闭
服务器地址	ezcloud.uniview.com
注册码	XXXXXXXXXXXXXXXXXXXX
设备状态	在线 <input type="button" value="注销"/>
用户名	f00432
设备名称	vms2-7-8
服务协议	http://ezcloud.uniview.com/doc/termsofservice.html
设备网络类型检测	<input type="button" value="检测"/>
扫一扫	

查看客户端侧的NAT类型：在CS客户端的登录页面选择<云账号登录>，登录后点击<网络检测>按钮查看。



11 RTSP协议接入设备

用RTSP协议接入IPC或NVR实现实况业务。

1. 点击<添加>，完成所需设置。

编辑设备

接入协议:	自定义 ¹	* 自定义协议:	XX厂家IPC 编辑 ³
* 设备名称:	203.8.1.183	设备类型:	NVR
* 组织名称:	根组织	* IP域名:	203.8.1.183
* 用户名:	admin	备注:	
密码:		
* 所属服务器:	VMS		
* 远程通道总数:	1 ²		

* 选择远程通道:

全选

远程通道1

说明: 1填写远程通道总数后, 默认全选;

2. 请确保勾选的首个通道可正常实况; 否则设备无法上线。

确定 取消

说明:

- “接入协议”：必须设置为“自定义”。
- “远程通道数”：IPC为1；NVR为实际通道数。必须确保勾选的首个通道的实况正常，否则设备无法上线。

2. 点击<编辑>，继续其他设置。

编辑协议

* 协议名称:

* 端口:

传输协议:

主码流: 开启 关闭

* 资源路径: rtsp://<ip>:<port>/

辅码流: 开启 关闭

* 资源路径: rtsp://<ip>:<port>/

第三流: 开启 关闭

示例: rtsp://<ip地址>:<端口号>/<资源路径>

单通道添加:
rtsp://192.168.0.1:554/unicast/c1/s0/live

多通道添加:
rtsp://192.168.0.1:554/unicast/c[%C]/s0/live; 添加指定的所有通道
rtsp://192.168.0.1:554/unicast/c[%C+1]/s0/live; 添加指定的所有通道偏移加1
rtsp://192.168.0.1:554/unicast/c[%C-1]/s0/live; 添加指定的所有通道偏移减1
[%C=N]; %C表示匹配选择的远程通道号, N表示通道的偏移量



说明:

“资源路径”：请根据接入设备厂家定义的格式填写后半部分。图中仅为示例。

3. 添加成功并成功上线后，可在客户端上正常实况。

12 自定义多源数据融幕

自定义多源数据融幕显示的数据模块和视图排版。



说明:

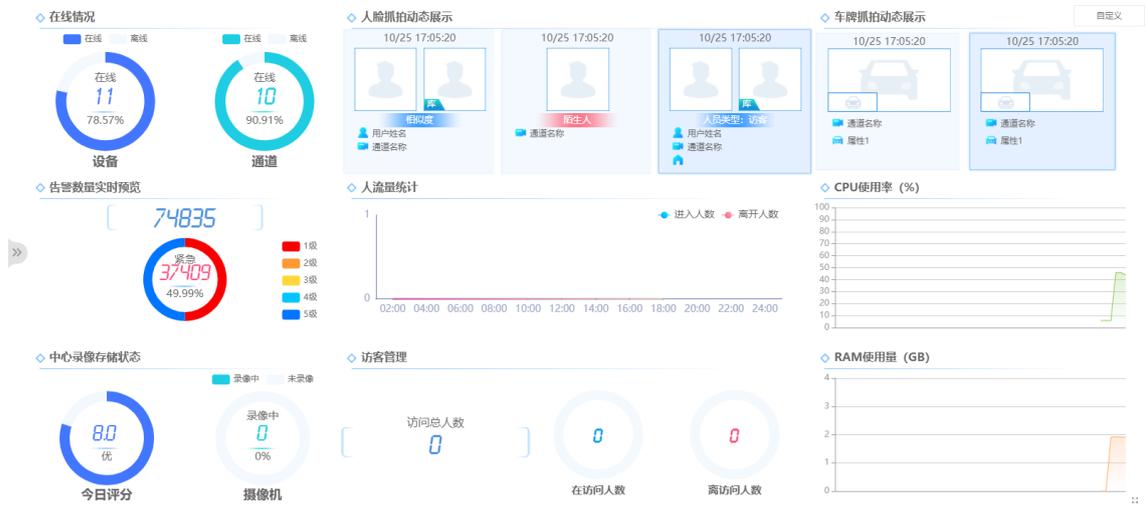
下图仅为示例。实际显示的数据模块与设备型号、软件版本等因素有关。请以实际为准。

1.

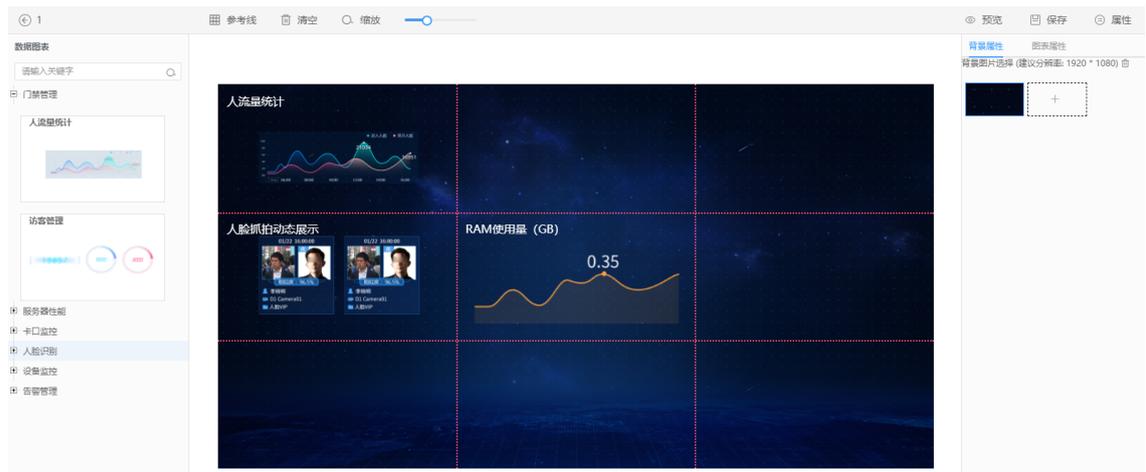
在首页点击页面右侧的展开按钮



2. 单击右上角的<自定义>按钮。



3. 点击  新增模板并设置模板名称。
4. 在左侧[数据图表]区域框，点击展开各模块找到要展示的模块，拖至右侧面板上，如“在线情况”、“中心录像存储状态”、“告警数量实时预览”。



- 参考线：选择或自定义面板上显示的红色虚线。
 - 清空：点击清空面板上的所有数据模块。
 - 缩放：左右拖动调整面板显示比例。
 - 预览：点击查看效果。
 - 保存：点击保存设置。
 - 属性：设置背景属性（面板背景）和图表属性（是否显示图标标题，如“在线情况”）。
5. 完成设置后，点击<保存>。
 6. 要启用模板，将鼠标放置在模板缩率图上，勾选右上角的勾（蓝色底表示启用成功）。



12.1 数据图表

门禁管理

- 人流量统计：按整点统计当日进入人数和离开人数，鼠标放置在折线上可查看对应时刻的数据。该折线图每2小时刷新一次。
- 访客统计：按日统计当日的访客总人数和当前在场人数。

服务器性能

- RAM使用量：查看服务器随机存取存储器使用量，打开多源数据融幕后自动开始统计，最多显示180秒的统计结果。鼠标放置在图表上可查看对应时刻的统计信息。
- CPU使用率：同上。

卡口监控

展示车牌抓拍动态，可展示抓拍时间、图片和通道名称等。

人脸识别

可显示人脸匹配数据：时间，相似度，人脸库图片，抓拍图片，名称，通道名称等。

设备监控

- 在线情况：通过饼状图展示当前在线和离线的设备/通道情况，可将光标放置在饼状图上查看当前在线和离线设备/通道的百分比及具体数值。鼠标单击设备饼状图可以跳转至[运维统计 > 设备统计 > 设备状态](#)页面，查看详细设备信息；鼠标单击通道饼状图可以跳转至[设备管理 > 通道 > 编码通道](#)页面，查看详细通道信息。
- 中心录像存储状态：通过饼状图展示当前摄像机通道的录像存储状态录像中/未录像，光标放在饼图上可查看百分比；使用鼠标单击摄像机饼状图可以跳转至[运维统计 > 服务器统计 > 录像状态](#)页面，查看详细的录像情况。该饼状图数据半小时刷新一次。

告警管理

通过饼状图不同颜色展示当前不同等级告警及其数量，光标放在饼图上可查看不同等级告警的数量及其百分比；使用鼠标单击饼状图可以跳转至[运维统计 > 日志查询 > 设备报警日志](#)页面，查看详细的告警信息。该饼状图数据1分钟刷新一次。