快速配置工具

使用说明书

V1.1.4

前言

符号约定

在本文档中可能出现下列标识，代表的含义如下。

标识	说明
危险	表示有高度潜在危险，如果不能避免，会导致人员伤亡或严重伤害。
警告	表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
注意	表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
防静电	表示静电敏感的设备。
当心触电	表示高压危险。
激光辐射	表示强激光辐射。
风扇警告	表示危险运动部件，请远离运动风扇叶片。
当心机械伤人	表示设备部件机械伤人。
窍门	表示能帮助您解决某个问题或节省您的时间。
说明	表示是正文的附加信息，是对正文的强调和补充。

修订记录

版本号	修订内容	发布日期
V1.1.4	● 新增“安装与卸载”、 “对讲设备”、“安卓广告机设备”、“楼宇配置”章节。 ● 更新文档软件的 UI 界面。 ● 修改“CGI 协议”、“门禁设备”章节。 ● 调整“开启 35114 协议”、“配置国密协同服务器”章节位置。	2020.08
V1.1.3	● 新增批量配置设备信息、一键授予设备 License 和一键恢复设备 License 为出厂状态、门禁配置说明。 ● 删除“配置模板”章节。 ● 优化产品授权、证书管理、重置密码描述。	2020.06
V1.1.2	文档模板修改为通用模板。	2020.04
V1.1.1	设置界面新增升级传输速度。	2020.03
V1.1.0	● 新增“设置视频 P/N 制式”章节。 ● 更新“应用模板”和“恢复设置”章节。	2020.01

版本号	修订内容	发布日期
V1.0.9	● 新增“工具配置”章节。 ● 删除“云升级”章节。	2019.09
V1.0.8	● 更新“密码重置”章节。 ● 更新“证书管理”章节。	2019.05
V1.0.7	● 新增“密码重置”章节。	2019.03
V1.0.6	● “加密授权”功能变更为“产品授权”功能。 ● 新增“研发授权”和“维修授权”章节。	2019.02
V1.0.5	● 系统配置中增加加密授权和证书管理功能描述。 ● 系统配置其他功能描述中更新截图。	2018.11
V1.0.4	● 系统配置界面的密码重置，单击“密码重置”时，新增提示框。 ● 云升级界面，单击“批量下载”和“升级检测”，新增提示框。 ● 系统配置界面新增视频文件密码找回功能。	2018.04
V1.0.3	● 新增“网络安全协议”、“云升级”章节。	2017.09
V1.0.2	● 更新“日常操作”章节。	2017.03
V1.0.1	● 新增“卸载”描述。 ● 更新“日常操作”章节。	2016.11
V1.0.0	● 新增“法律声明”章节。 ● 更新“日常操作”章节。	2016.02

目录

前言 II
第 1 章 概述 1
第 2 章 安装与卸载 2
2.1 安装 2
2.2 卸载 4
第 3 章 界面介绍 6
第 4 章 基本操作 8
4.1 添加设备 8
4.1.1 单台添加 8
4.1.2 批量添加 9
4.2 初始化设备 10
4.3 修改 IP 13
4.3.1 单台修改 13
4.3.2 批量修改 14
4.4 升级设备 15
4.4.1 单台升级 15
4.4.2 批量升级 15
4.5 配置设备 16
4.5.1 监控设备 16
4.5.2 门禁设备 21
4.5.3 对讲设备（VTH/VTO/VTS） 23
4.5.4 安卓广告机设备 32
4.6 配置系统信息 33
4.6.1 校准设备时间 33
4.6.2 重启设备 35
4.6.3 恢复设置 35
4.6.4 修改设备密码 37
4.6.5 视频配置 38
4.6.6 批量表单操作 38
4.6.7 产品授权 39
4.6.8 证书管理 41
4.7 重置密码 46
4.7.1 批量重置 46
4.7.2 单台重置 48
4.8 楼宇配置 49
4.9 CGI 协议 50
4.9.1 通过 CGI 配置信息 50
4.9.2 通过 CGI 批量配置信息 51
4.9.3 通过表单配置信息 51
4.10 查看帮助文档 52
4.11 查看工具版本 52
第 5 章 工具配置 53
附录 1 验证 35114 协议 55

附录 1.1 登录设备 55
附录 1.2 添加远程设备 56
附录 1.3 实时预览 56
附录 2 法律声明 57
附录 3 网络安全建议 58

第 1 章 概述

快速配置工具（英文名称为 ConfigTool，以下简称工具）主要用于配置和维护设备，如 IPC、NVR 和门禁设备等，主要提供如下功能：

- 初始化设备。
- 修改设备的 IP 地址。
- 升级设备。
- 配置监控设备的编码参数、视频参数、监视模式；配置门禁设备不同通道的卡号反转、TCP 端口号、日志记录等信息；配置对讲设备的设备信息、物理信息、SIP 服务器信息；支持安卓广告机的 APP 配置、Android 调试、导出日志。
- 校准设备时间、重启设备、将设备设置恢复为默认设置、修改设备密码、重置设备密码、设置设备的视频制式、更新设备 License 等。
- 配置楼宇的 VTO/VTH 设备信息。
- 通过 CGI 批量配置设备信息或通过表单配置设备信息。

注意

请勿将本工具和设备故障诊断工具或 SmartPSS、SmartPSS Plus 同时使用，否则可能会导致设备搜索异常。

第 2 章 安装与卸载

介绍安装和卸载 ConfigTool 的操作过程。

2.1 安装

前提条件

请联系技术支持获取 ConfigTool 安装包。

具体步骤

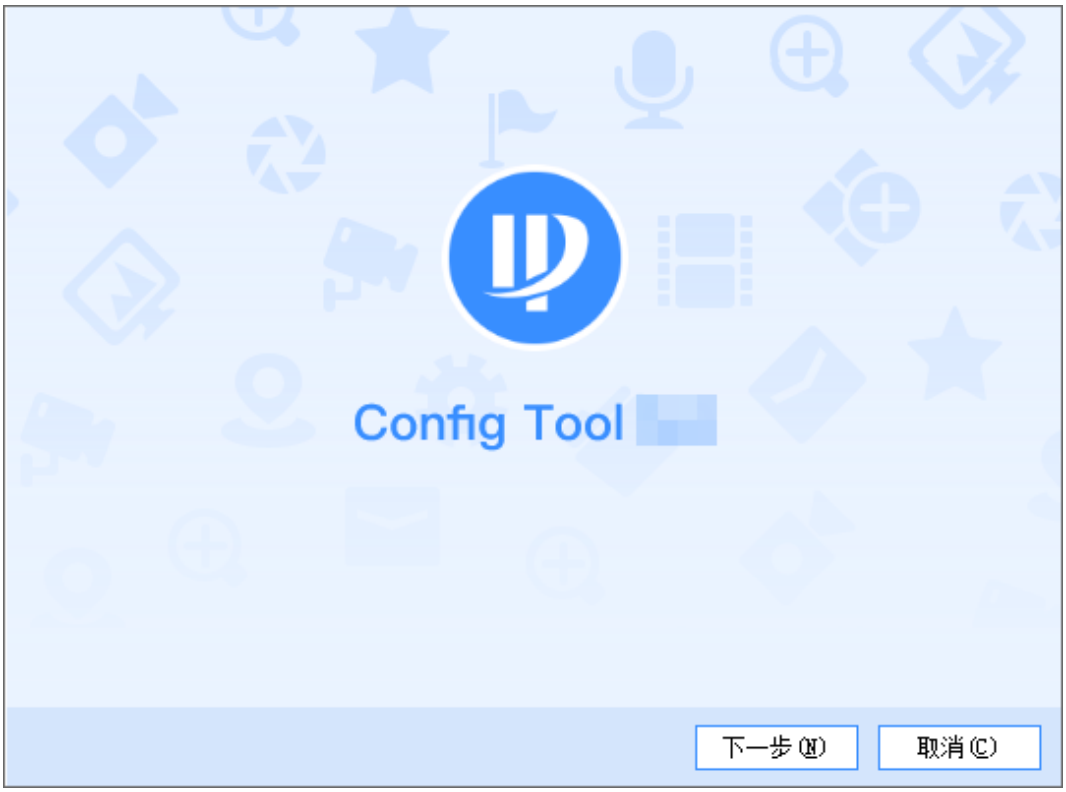
步骤1　双击 ConfigTool 安装包，系统弹出安装语言对话框。

步骤2　选择安装语言，并单击“OK”。

图2-1 弹出语言对话框

步骤3　单击“下一步”。

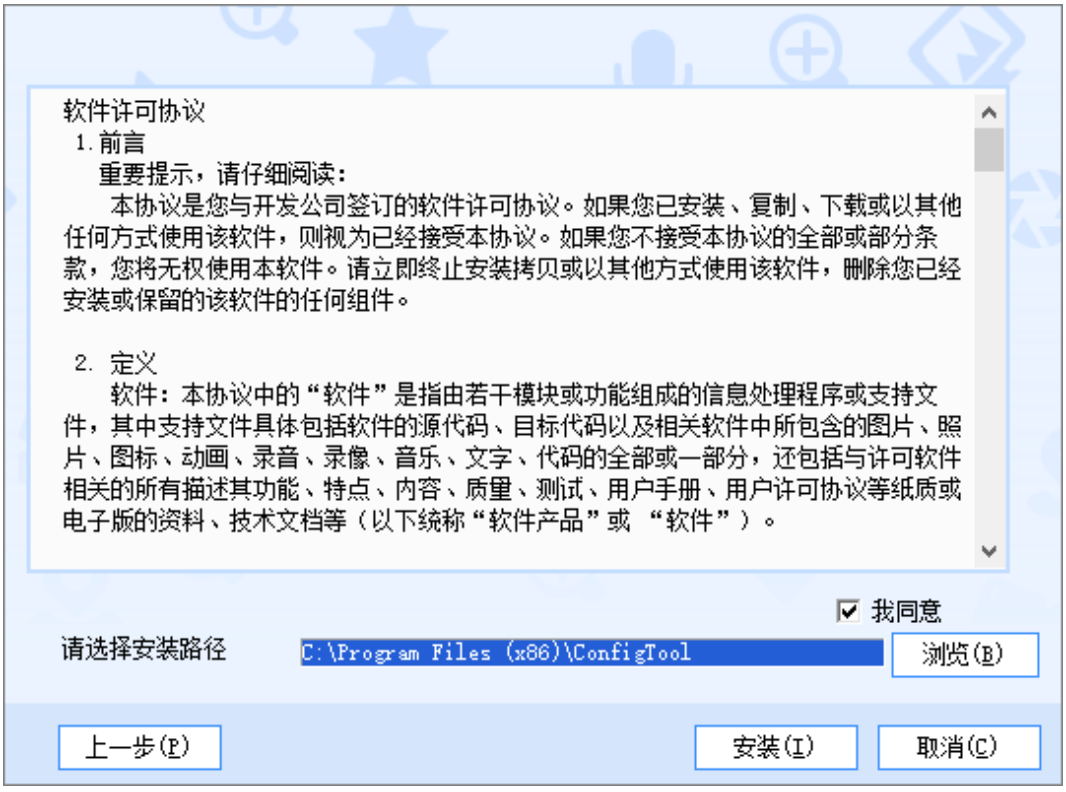
图2-2 安装 ConfigTool5.0



步骤4　阅读软件许可协议，选择“我同意”。单击“浏览”，选择安装路径。

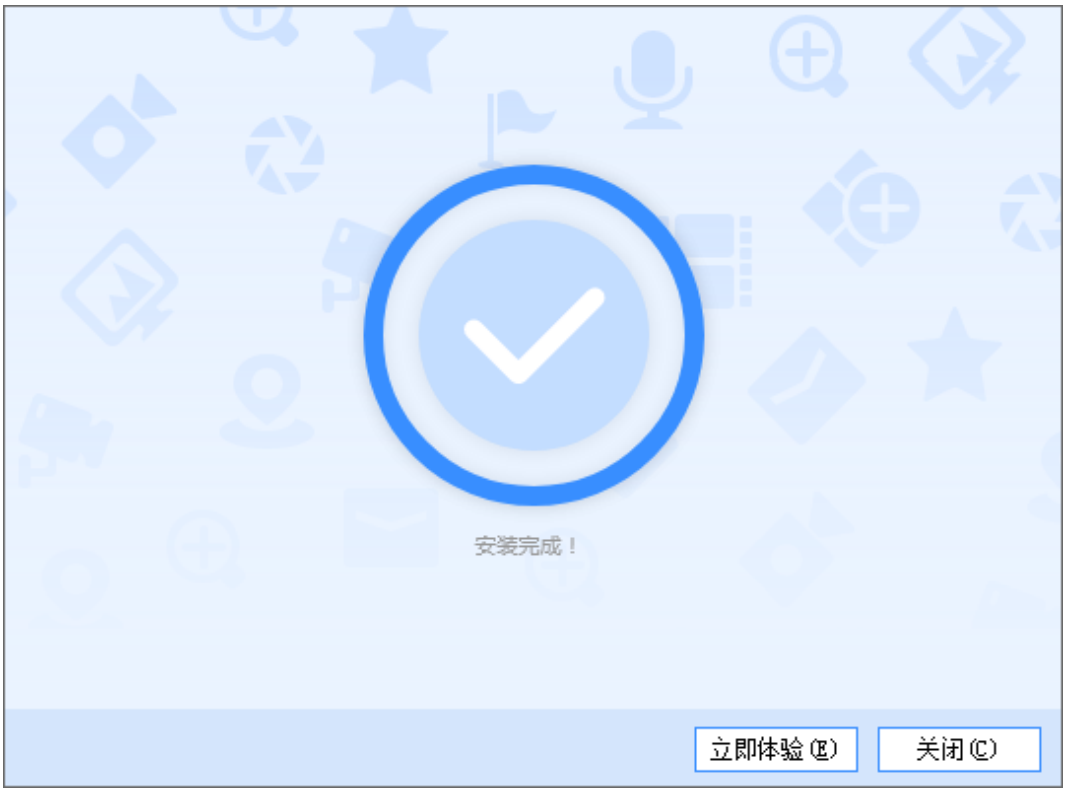
步骤5　单击“安装”，系统开始安装 ConfigTool。

图2-3 选择安装路径



步骤6　单击“立即体验”，完成安装并开启工具。单击“关闭”，完成安装并关闭工具。

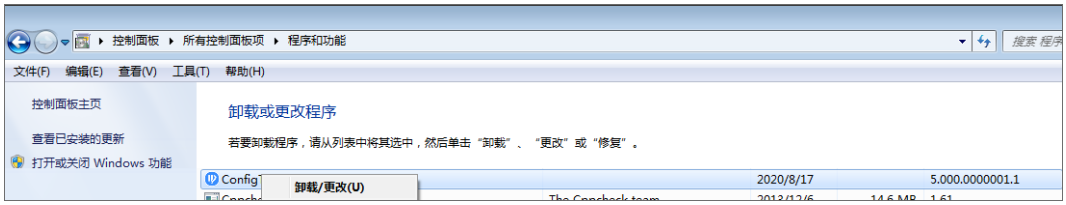
图2-4 安装完成



2.2 卸载

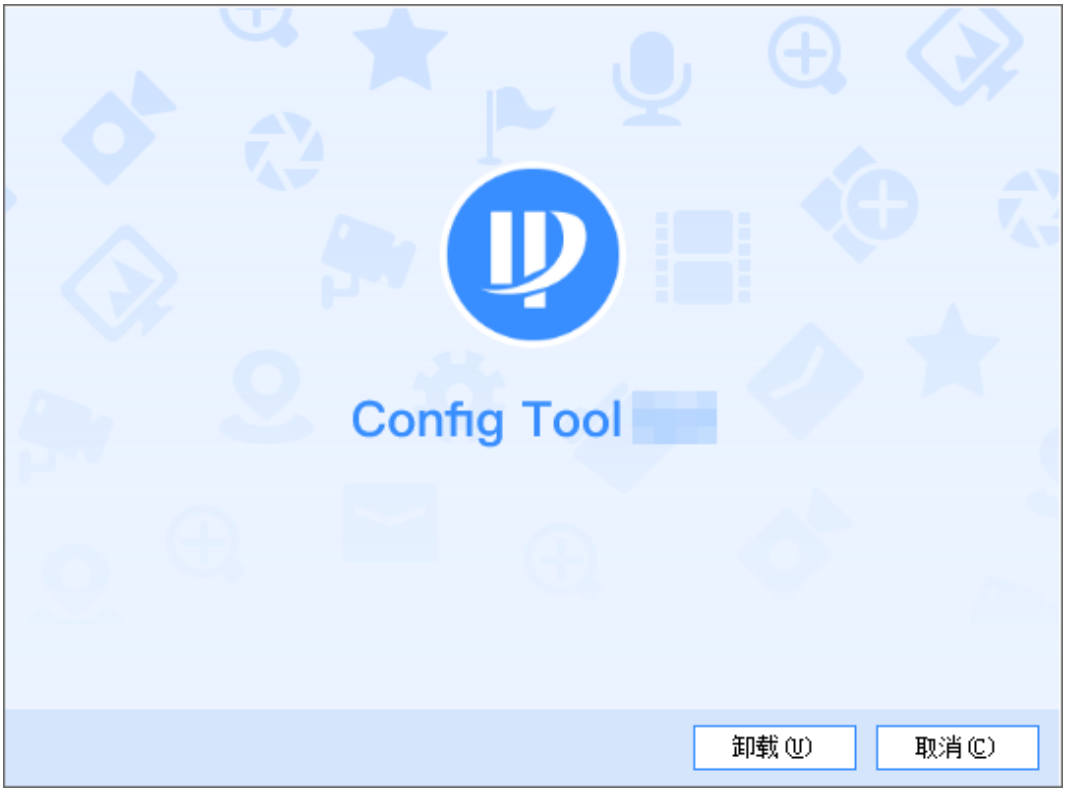
步骤1　打开控制面板，单击“ConfigTool”，右键选择“卸载/更改”。

图2-5　打开控制面板



步骤2　单击“卸载”。根据提示完成操作。

图2-6 卸载 ConfigTool



第 3 章 界面介绍

工具主界面如图 3-1 所示，详细说明请参见表 3-1。

说明

- 启动工具后，工具会自动按照“搜索设置”里设置的搜索方式搜索设备。
- 首次启动工具，工具自动搜索与 PC 处于同一网段的设备。

图3-1 工具主界面

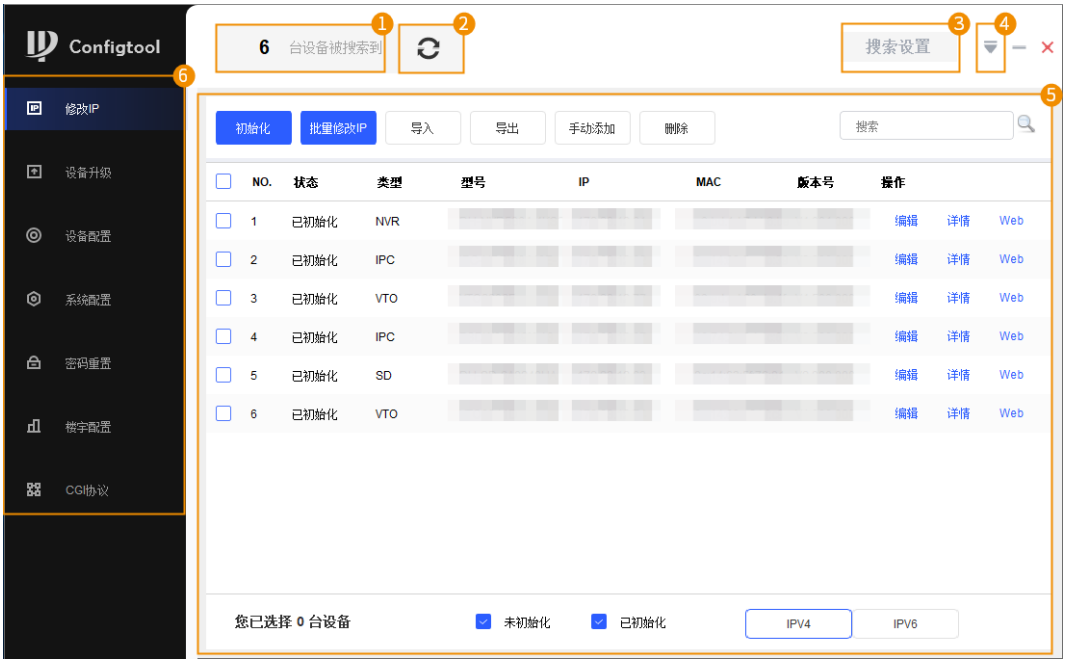


表3-1 主界面介绍

序号	名称	说明
1	-	显示搜索到的设备数量。
2	刷新	使用最后一次的搜索设置重新搜索设备。
3	搜索设置	搜索与工具所在 PC 同一网段的设备或通过设置搜索范围搜索设备。
4	关于	查看帮助文档、工具版本、开源声明、软件许可协议信息，以及配置工具登录设备的模式和升级设备相关参数。
5	功能模块	提供菜单功能。

序号	名称	说明
6	菜单栏	• ：主要用于添加设备到工具、初始化设备和修改设备 IP 地址等。 • ：用于升级设备。 • ：配置监控设备的编码参数、视频参数、监视模式；配置门禁设备不同通道的卡号反转、TCP 端口号、日志记录等信息；配置对讲设备的设备信息、物理信息、SIP 服务器信息；支持安卓广告机的 APP 配置、Android 调试、导出日志。 • ：主要用设置设备时间、重启设备、恢复设备配置为默认配置、导出设备配置到本地、导入配置到设备、设置视频 P/N 制式、更新设备 License、设备证书管理等。 • ：用于重置设备密码。 • ：通过模板填写 VTO/VTH 设备详细信息，将设备信息导入到快速配置工具。 • ：CGI（Common Gateway Interface，公共网关接口）。通过 CGI 批量配置设备信息或通过表单批量配置设备信息。

第 4 章 基本操作

4.1 添加设备

单台或者批量添加设备到工具，请根据实际情况选择合适的添加方式。

说明

请确保设备和安装工具的 PC 间网络互通，否则工具无法搜索到设备。

4.1.1 单台添加

当需要添加单台设备时，可选择此添加方式。

步骤1　在菜单栏单击 修改IP，然后单击“手动添加”。

步骤2　选择添加方式，然后填写设备参数。

步骤3　单击“确定”。

添加的设备显示在设备列表中。

图4-1 填写设备信息

表4-1 设备参数说明

添加方式	参数	说明
IP 地址	IP 地址	添加设备的 IP 地址。
	用户名	登录设备的用户名和密码。
	密码	
	端口	设备的端口号。
序列号（仅支持 P2P 功能设备可用）	序列号	设备的序列号。 **说明** ● 设备需要接入公网。 ● 中文的设备只能用中文的程序添加。
	用户名	登录设备的用户名和密码。
	密码	

4.1.2 批量添加

当需要添加多台设备时，通过搜索或者模板批量添加设备。

- 已知设备所在网段时，可以通过搜索添加设备，详细介绍请参见“4.1.2.1 搜索添加”。
- 已有设备型号、IP 地址、端口号和 MAC 地址等数据时，可以通过模板导入设备，详细介绍请参见“4.1.2.2 通过模板添加”。

4.1.2.1 搜索添加

通过搜索批量添加与 PC 同一网段或者其他网段的设备。

步骤1 单击“搜索设置”。

步骤2 根据实际情况选择搜索设备的方式。

- 搜索与工具所在 PC 同一网段的设备。

1. 选择“当前网段搜索”。
2. （可选）填写登录设备的用户名和密码。

- 通过设置搜索网段搜索设备。

1. 选择“其他网段搜索”
2. 设置“起始 IP”、“结束 IP”。
3. （可选）填写登录设备的用户名和密码。

说明

- 当同时选择“当前网段搜索”和“其他网段搜索”时，同时搜索当前网段和设置网段的设备。
- 无论是否填写登录设备的用户名和密码，均可以添加设备。如果正确填写设备用户名和密码，执行其他需要登录的操作（例如配置设备编码参数）时，工具将匹配此处填写的用户名和密码自动登录设备，直接进入操作界面，否则届时需填写正确的用户名和密码重新登录设备才能操作。

步骤3 单击“确定”，开始搜索设备。

添加的设备显示在设备列表中。

图4-2 设置搜索条件

说明

关闭工具时会保存设置的搜索条件，重新开启工具时会启用上次保存的设置。

4.1.2.2 通过模板添加

在设备信息模板填写需要添加到工具的设备信息，然后通过导入设备信息模板将设备添加到工具。通过模板一次最多添加 1000 台设备。

步骤1　导出设备信息模板。在菜单栏单击 修改IP，在设备列表选择任意设备，单击“导出”，导出设备信息模板到本地。

步骤2　打开设备信息模板，将信息修改为需要添加到工具的设备信息。

步骤3　导入设备信息模板到工具。在菜单栏单击 修改IP，单击“导入”，导入设备信息到工具。

导入的设备显示在设备列表中。

注意

请先关闭模板文件，再使用模板文件导入设备，否则会导入失败。

4.2 初始化设备

单台或者批量初始化设备。

说明

- 部分设备支持初始化。
- 只能对局域网内的设备进行初始化。
- 未初始化设备不能进行任何操作，同时其他界面不显示未初始化设备，请先完成设备初始化，再对设备操作，例如升级设备等。

步骤1　在菜单栏单击 修改IP，在设备列表选择未初始化的设备，单击“初始化”。

步骤2　在弹出的对话框选择需要初始化的设备，然后单击“初始化”。

图4-3 设备初始化（1）

步骤3　设置设备初始化参数，单击“下一步”。

说明

- 不同型号设备的界面显示可能不同，请以实际为准。
- 若不预留手机号码，忘记密码时只能通过发送 XML 文件方式重置密码，详细介绍请参见“4.7 重置密码”。
- 批量初始化时将根据第一台设备支持的密码重置方式来进行初始化设置。

图4-4 设备初始化（2）

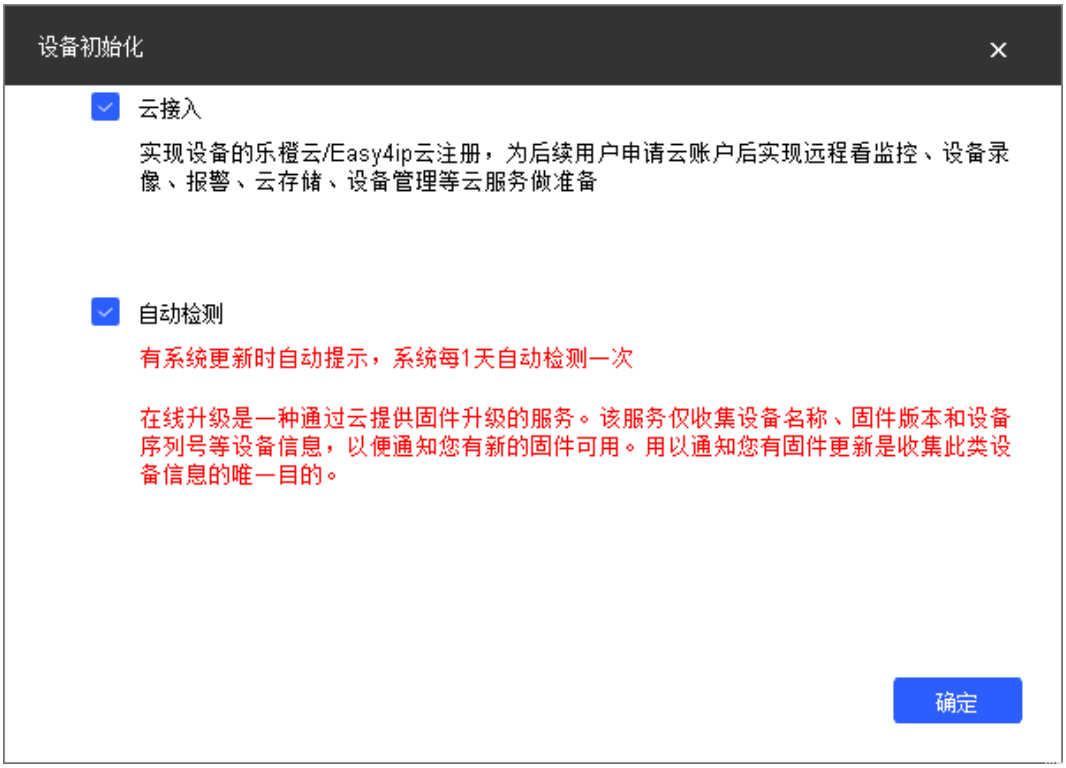
表4-2 设备参数说明

参数	说明
用户名	用户名默认为 admin。
新密码	设备不同，密码长度不同。输入设备的新密码。新密码可设置为 6 位纯数字，或 8 位～32 位必须由数字、字母和特殊字符（除“'”、“″”、“;”、“:”、“&”外）三种类型中的至少两种组成。请根据密码强弱提示设置高安全性密码。
确认密码	确认输入的新密码。
预留手机	默认已选择，输入的手机号码将用于密码重置。

步骤4　请根据界面提示和您的实际需求为设备选择 “自动检测”功能和“云接入”功能，单击“确定”，然后根据提示完成初始化操作。

初始化成功完成后，在设备列表设备的状态显示为“已初始化”。

图4-5 根据实际需求选择功能



4.3 修改 IP

单台或者批量修改设备的 IP 地址。

- 当设备较少或者设备的登录密码不相同时，可以单台修改设备的 IP 地址。
- 当设备较多且设备的登录密码相同时，可以批量修改设备的 IP 地址。

4.3.1 单台修改

当需要修改单台设备 IP 时，可选择此修改方式。

步骤1　在菜单栏单击

。

步骤2　单击需要修改 IP 的设备对应的

。

步骤3　根据实际情况选择 IP 地址的修改方式。

- DHCP 模式：当网络中存在 DHCP 服务器时，设置“模式”为“DHCP”，则设备自动从 DHCP 服务器获取 IP 地址。
- 手动模式：设置“模式”为“静态”，并填写设备的“目标 IP”、“子网掩码”和“网关”，则设备的 IP 地址修改为设置的 IP 地址。

步骤4　单击“确定”。

图4-6 修改设备 IP

4.3.2 批量修改

当需要修改多台设备的 IP 时，可通过批量修改功能进行修改。

步骤1　在菜单栏单击 修改IP，选择需要修改 IP 的设备，单击“批量修改”。

步骤2　根据实际情况选择设置 IP 地址的模式。

- DHCP 模式：当网络中存在 DHCP 服务器时，设置“模式”为“DHCP”，则设备自动从 DHCP 服务器获取 IP 地址。
- 手动模式：设置“模式”为“静态”，并填写设备的“起始 IP”、“子网掩码”和“网关”，则在设备列表从上向下设备 IP 地址从起始 IP 开始依次递增修改。

说明

选择“同一 IP”，将选中的多台设备设置为同一个 IP 地址，建议统一设置出厂默认 IP 时使用。

步骤3　单击“确定”。

图4-7 批量修改设备 IP

4.4 升级设备

支持单台或者批量升级设备。

升级设备的速度与升级包容量有关，具体情况如下：

- 当升级包容量＜100MB 时，工具自动按照 1KB/次的传输速度传输升级包，传输速度不支持修改。
- 当升级包容量≥2GB 时，工具自动按照 16KB/次的传输速度传输升级包，传输速度不支持修改。
- 当 100MB≤升级包容量＜2GB 之间，工具默认按照 1KB/次的传输速度传输升级包，如需提升传输速度，请将传输速度设置为 16KB/次，详细介绍请参见“4.9.1”。

楼宇、门禁设备、对讲设备和安卓广告机设备升级需求按照默认的 1KB/次升级，切换不生效。

说明

升级过程中如果设备断线，工具会提示断线，设备可能会重启。

- 如果升级进度不足 50%，表示升级包传输未完成，设备重连后，请重新搜索设备并重新升级设备。
- 如果升级进度超过 50%，表示升级包已经完成传输，设备会升级成功，设备重连并重新搜索后显示的是设备升级后的版本。

4.4.1 单台升级

当需要升级单台设备时，可选择此升级方式。

步骤1　在菜单栏单击

。

步骤2　单击需要升级的设备对应的 ，选择升级文件，并单击 。

步骤3　单击“升级”，开始升级设备。

升级完成后，设备自动重新启动。

4.4.2 批量升级

当需要将多台设备批量升级到同一软件版本，可选择此升级方式。

步骤1　在菜单栏单击

。

步骤2　在设备列表选择需要升级的设备，单击“批量升级”

说明

选择的设备必须是升级到同一个软件版本的设备。

步骤3　单击“打开”，选择升级文件。

步骤4　单击“确定”。

4.5 配置设备

4.5.1 监控设备

配置监控设备的编码参数、视频参数，以及配置设备的监视模式。

4.5.1.1 配置编码参数

配置摄像机的码流类型、编码模式、分辨率等参数。

步骤1　在菜单栏单击

。

步骤2　在设备列表双击要配置的监控设备或单击要配置的监控设备，然后单击“获取设备信息”。

步骤3　（可选）如果提示登录设备，请在“登录”对话框填写登录设备的用户名和密码，单击“确定”。

步骤4　在“编码配置”页签下，配置主码流、辅码流的编码参数。

步骤5　单击“确定”。

说明

不同设备的编码参数可能不同，请以实际界面显示为准。

表4-3 编码参数说明

参数	说明
通道	选择需要配置的设备通道。
码流类型	主码流包括普通、动检、报警三种，辅码流只支持普通。
编码模式	视频的编码模式。不同设备支持的视频编码模式不同。部分视频编码模式的含义如下，详细介绍请参见设备的使用说明书。 ● H.264：Main Profile 编码方式。 ● H.264B：Baseline Profile 编码方式。 ● H.264H：High Profile 编码方式。 ● H.265：Main Profile 编码方式。 ● MJPG：该编码模式下视频画面需要较高的码流值才能保证图像的清晰度，为了使视频画面达到较佳效果，建议使用相应参考码流值中的最大码流值。
码流控制	视频的码流控制方式，包括如下选项。 ● 固定码流：码流变化较小，码流保持在设置的码流值附近变化。 ● 可变码流：码流会随着监视场景等发生变化。 **说明** 当“编码模式”设置为“MJPG”时，码流控制方式只能是固定码流。
帧率	视频每秒包含的帧数。帧率越高，图像越逼真和流畅。
分辨率	视频的分辨率。不同设备的最大分辨率可能不同，请以实际界面显示为准。
图像质量	当“码流控制”设置为“可变码流”时，支持设置该参数。 数值越大，视频画面质量越好。

参数	说明
码流	根据实际场景选择适合的码流。
音频/视频使能	选择视频使能后，才能用辅码流查看/下载录像，同时开启音频使能后，用辅码流查看/下载的录像才有声音。
音频编码	音频的编码模式。 设置的音频编码模式会对音频和语音对讲同时生效。
采样率	音频的采样频率。

步骤6　（可选）将配置应用到其他设备。

1. 单击“应用到...”，在设备导航树选择需要应用该配置的设备，单击“配置”。
   配置应用到设备。若应用成功，设备右侧显示✓；若失败，显示⚠。单击✓或⚠可查看详细信息。
2. 单击“返回”，返回到配置界面。

4.5.1.2 配置视频参数

配置普通、白天和夜晚三种模式的视频参数。视频参数的效果通过监视画面可以实时查看。

步骤1　在菜单栏单击

。

步骤2　在设备列表双击要配置的监控设备或单击要配置的监控设备，然后单击“获取设备信息”。

步骤3　（可选）如果提示登录设备，请在“登录”对话框填写登录设备的用户名和密码，单击“确定”。

步骤4　在“视频配置”页签设置视频参数。

说明

- 单击“恢复默认”，恢复设备默认参数。
- 在视频画面上滚动鼠标滚轮可以对视频画面进行电子放大，单击右键恢复图像默认大小。
- 单击视频窗口中的 ，可以全屏显示视频窗口；视频窗口全屏显示时，单击 或【ESC】按键，可以恢复到默认大小。

图4-8 视频配置

表4-4 视频参数说明

参数	说明
配置文件	选择设备的配置文件，包括白天、夜晚和普通。
通道	选择设备对应的通道。
颜色模式	视频画面的颜色模式，包括标准、艳丽和柔和三种模式。
亮度	通过线性的调节方式调节图像的整体亮度。值越大图像越亮，反之越暗。
对比度	调节图像的对比度。值越大图像明亮反差越大，反之越小。
伽马	通过非线性方式调节图像的亮度，提高图像的动态显示范围。伽马值越大，图像越亮，请根据实际情况调节图像的伽马值。
饱和度	调整颜色深浅。值越大彩色将越浓，反之越淡。该值不会影响图像的整体亮度。
日/夜模式	设置摄像机图像显示为彩色或者黑白模式。 包括如下选项： ● 彩色：摄像机图像显示为彩色图像。 ● 自动：根据环境亮度摄像机自动选择显示为彩色图像或者黑白图像。 ● 黑白：摄像机图像显示为黑白图像。
背光补偿模式	● 关闭：关闭背光补偿模式。 ● 背光补偿：在逆光环境下，背光补偿能避免在逆光环境下拍摄主体较暗部分出现剪影的现象。 ● 宽动态：在光照对比强烈的环境下，开启宽动态能抑制过亮的区域，补偿过暗的区域，使画面整体呈现一个较为清楚的状态。 ● 强光抑制：强光抑制能把强光部分弱化，达到光线平衡。

参数	说明
通道名	设置摄像机的通道名称，不能为空字符。

步骤5　（可选）设置辅助聚焦。

说明

当需要微调设备焦距时，执行此步骤。

1. 单击“辅助聚焦”。
   工具显示“辅助聚焦”界面。

图4-9 辅助聚焦

2. 将设备调到最小焦距，并单击“开始采样”，同时手动将设备调到最大焦距。
   工具显示开始采样后的界面。

图4-10 开始采样

3. 单击“开始微调”。
   工具显示最佳区域，通过手动调焦直到焦距指示线进入最佳区域。

说明

图中红色线为当前画面的清晰度值，绿色线为焦距从最小到最大的清晰度值。

4. 单击“停止”，停止焦距微调。

图4-11 最终效果

步骤6 （可选）将配置应用到其他设备。

1. 单击“应用到...”，在设备导航树选择需要应用该配置的设备，单击“配置”。配置应用到设备。若应用成功，设备右侧显示✓；若失败，显示⚠。单击✓或⚠可查看详细信息。
2. 单击“返回”，返回到配置界面。

4.5.1.3 配置监视模式

配置如下任意一种监视模式：

- 按普通模式监视。
- 全时段按白天或夜晚模式监视。
- 不同时段使用不同的模式监视，例如 8:00～17:00 使用白天模式监视，其他时间使用夜晚模式监视。

步骤1 在菜单栏单击

。

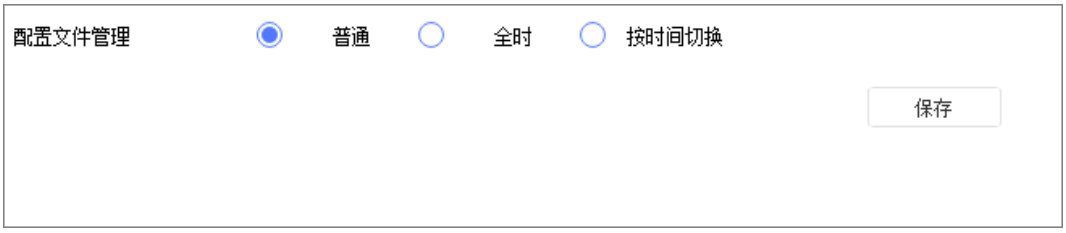
步骤2 在设备列表双击监控设备或单击要配置的监控设备，然后单击“获取设备信息”。

步骤3 （可选）如果提示登录设备，请在“登录”对话框填写登录设备的用户名和密码，单击“确定”。

步骤4 在“配置文件管理”页签配置监视模式。

- 按普通模式监视。选择“普通”，则设备按照普通配置监视。

图4-12 配置按照普通模式监视



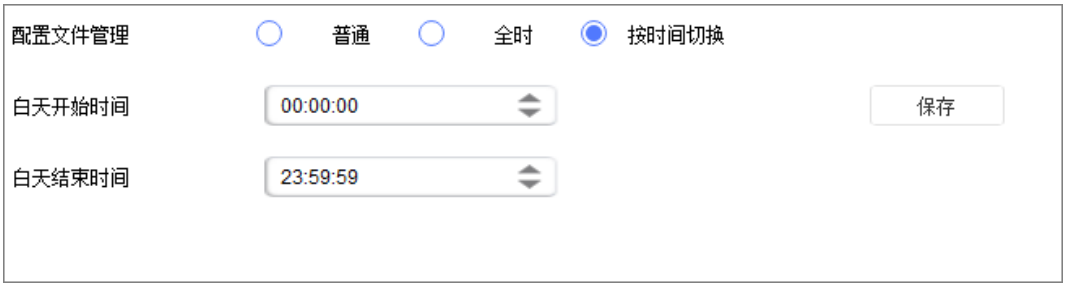
- 全时段按白天或夜晚模式监视。选择“全时”，将“总是使用”设置为“白天”，则设备始终按照白天模式监视；设置为“夜晚”，则设备始终按照夜晚模式监视。

图4-13 配置全时段按白天或夜晚模式监视

- 不同时段使用不同的模式监视。选择“按时间切换”，设置白天的开始和结束时间，例如设置白天为 8:00～17:00，则该时间段按照白天模式监视，其余时间按照夜晚模式监视。

步骤5　单击“保存”，完成配置。

图4-14 配置不同时段使用不同的模式监视



步骤6　（可选）将配置应用到其他设备。

1. 单击“应用到...”，在设备导航树选择需要应用该配置的设备，单击“配置”。配置应用到设备。若应用成功，设备右侧显示✓；若失败，显示⚠。单击✓或⚠可查看详细信息。
2. 单击“返回”，返回到配置界面。

4.5.2 门禁设备

配置门禁控制器的卡号处理规则、修改门禁设备端口号和获取门禁设备操作日志等。

说明

不同门禁设备支持配置的参数可能不同，请以实际界面为准。

步骤1　在菜单栏单击

。

步骤2　在设备列表双击门禁设备或单击要配置的门禁设备，然后单击“获取设备信息”。

步骤3　（可选）如果提示登录设备，请在“登录”对话框填写登录设备的用户名和密码，单击“确定”。

步骤4　配置门禁参数。

图4-15 配置门禁参数

表4-5 门禁参数说明

参数	说明
通道	选择门禁设备通道，“卡号反转”设置将在该门禁设备通道生效。
卡号反转	设置门禁控制器的卡号处理规则，默认为“卡号正序”。 当从读卡器读取的卡号与实际卡号不同时，请选择“卡号反序”或“HID”，使读卡器读取的卡号和实际卡号相同。 ● 卡号反序：当门禁控制器和第三方读卡器配合使用，且从读卡器读取的卡号和实际卡号字节顺序相反，例如从读卡器读取的卡号是十六进制 12345678，实际卡号是十六进制 78563412，选择“卡号反序”，使读卡器读取的卡号和实际卡号相同。 ● HID：当门禁控制器和第三方 HID 韦根读卡器配合使用，且从读卡器读取的卡号和实际卡号不同，例如从读卡器读取的卡号是十六进制 1BAB96，实际卡号是 78123456，选择“HID”，使读卡器读取的卡号和实际卡号相同。
TCP 端口号	修改设备端口号，并单击“保存”。修改后，添加该设备到平台时，需要填写修改后的端口号。
日志记录	单击“获取”，在弹出的对话框选择保存路径，将获取设备的操作日志并保存到该路径。
读卡器序号	选择需要设置波特率和开启 OSDP 功能的读卡器。选择后，配置的波特率和 OSDP 功能将在该读卡器生效。
波特率	用于配置门禁控制器与读卡器之间的通信速率。提高波特率可以提升通信速率。波特率默认为 9600。
OSDP 使能	当门禁控制器与第三方读卡器配合使用，且两者之间使用 OSDP 协议通信时，请开启 OSDP 功能。开启后，门禁控制器与第三方读卡器才能正常通信。

步骤5 （可选）将配置应用到其他设备。

1. 单击“应用到...”，在设备导航树选择需要应用该配置的设备，单击“配置”。
   配置应用到设备。若应用成功，设备右侧显示✓；若失败，显示⚠。单击✓或⚠可查看详细信息。
2. 单击“返回”，返回到配置界面。

4.5.3 对讲设备（VTH/VTO/VTS）

- VTH：室内机。
- VTO：门口机。
- VTS：管理机。

4.5.3.1 VTO

步骤1　在菜单栏单击

。

步骤2　在设备列表双击 VTO 设备或单击要配置的 VTO 设备，然后单击“获取设备信息”。

步骤3　（可选）如果提示登录设备，请在“登录”对话框填写登录设备的用户名和密码，单击“确定”。

步骤4　配置 VTO 设备参数，单击“保存”。

图4-16 配置 VTO 设备参数

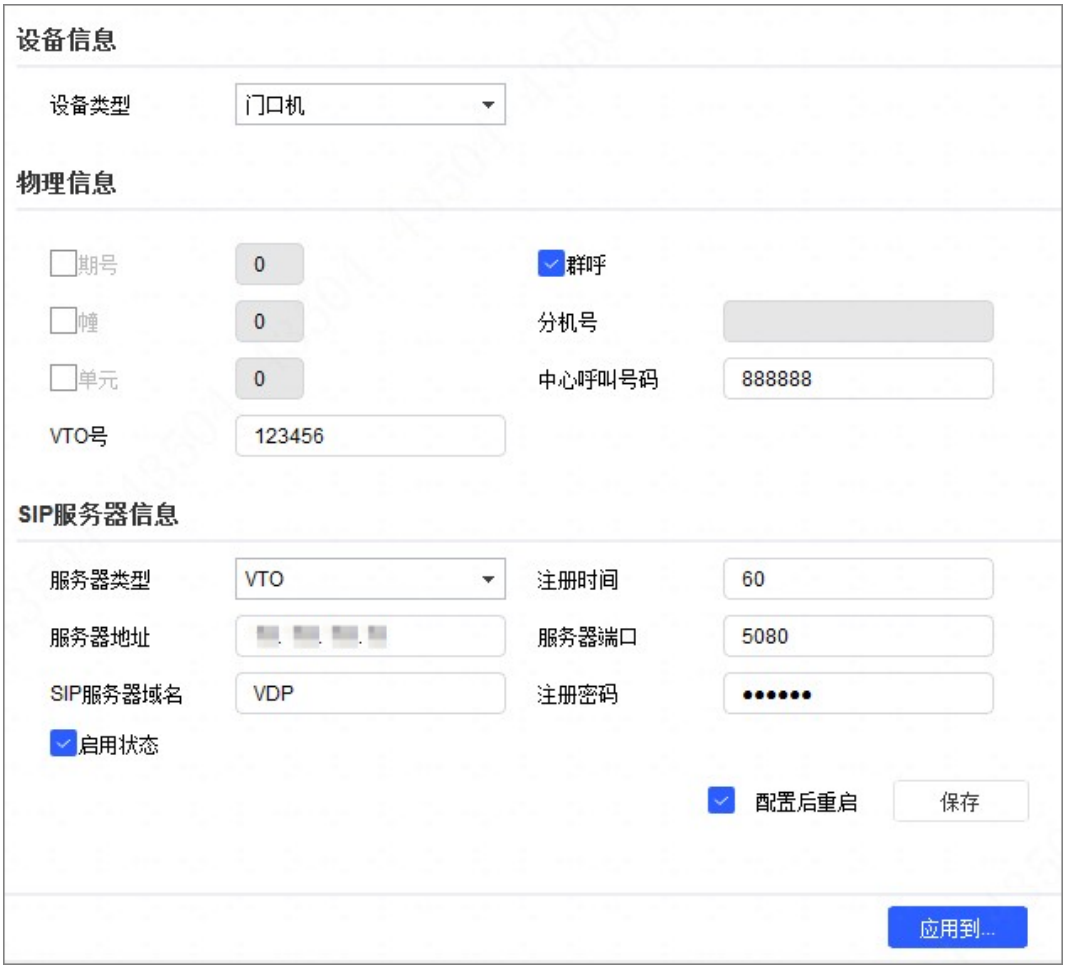


表4-6 配置 VTO 设备参数

参数		说明
设备类型		选择“门口机”或“围墙机”。
物理信息	期号	填写 VTO 设备所在期号。
	幢	填写 VTO 设备所在幢号。
	单元	填写 VTO 设备所在单元号。
	分机号	VTO 设备的分机号。

参数		说明
	中心呼叫号码	VTO 设备的中心呼叫号码，默认 888888。
	VTO 号	VTO 设备的 VTO 号。
SIP 服务器信息	服务器类型	选择/、VTO、私有服务器、VTNS 中转服务器类型。
	服务器地址	SIP 服务器的地址。
	SIP 服务器域名	SIP 服务器的域名。
	注册时间	SIP 服务器的注册时间。
	服务器端口	SIP 服务器的端口号。
	注册密码	SIP 服务器注册密码。
	启用状态	选择“启用状态”，开启 SIP 服务器。
	配置后重启	选择“配置后重启”，配置后重启设备。取消选择，配置后不重启设备。

步骤5　（可选）将配置应用到其他设备。

1. 单击“应用到...”，在设备导航树选择需要应用该配置的设备，单击“配置”。配置应用到设备。若应用成功，设备右侧显示✓；若失败，显示⚠。单击✓或⚠可查看详细信息。
2. 单击“返回”，返回到配置界面。

4.5.3.2 VTH

4.5.3.2.1 网络配置

步骤1　在菜单栏单击

。

步骤2　在设备列表双击 VTH 设备或单击要配置的 VTH 设备，然后单击“获取设备信息”。

步骤3　（可选）如果提示登录设备，请在“登录”对话框填写登录设备的用户名和密码，单击“确定”。

步骤4　在“网络配置”页签下，配置 VTH 设备本机设置、SIP 服务器参数。

步骤5　单击“确定”。

图4-17 网络配置

表4-7 本机配置参数

参数	说明
房间号	房间号码。
主机 IP	设置主机的 IP 地址。 **说明** • 选择“主室内机”，则默认该 IP 为主机，不用配置主机用户名、密码、IP 地址。 • 选择“从室内机”，则需配置主机用户名、密码、IP 地址。
主机用户名	填写主机的登录用户名。
主机密码	填写主机的登录密码。
SSH	选择“SSH”。 **说明** SSH，Secure Shell 的缩写，是一种安全的连接方式。

表4-8 SIP 服务器配置

参数	说明
服务器 IP	SIP 服务器的 IP 地址。
网络端口号	SIP 服务器的网络端口号。
注册密码	SIP 服务器的注册密码。
域名	SIP 服务器的域名。
用户名	SIP 服务器的登录用户名。
登录密码	SIP 服务器的登录密码。
启用状态	选择“启用状态”。

步骤6 （可选）将配置应用到其他设备。

1. 单击“应用到...”，在设备导航树选择需要应用该配置的设备，单击“配置”。配置应用到设备。若应用成功，设备右侧显示✓；若失败，显示⚠。单击✓或⚠可

查看详细信息。

2. 单击“返回”，返回到配置界面。

说明

任一模式下单击“应用到...”，只配置该模式下的参数。如果想应用全部，需切换页签重复配置。

4.5.3.2.2 网络终端

步骤1 在菜单栏单击 设备配置。

步骤2 在设备列表双击 VTH 设备或单击要配置的 VTH 设备，然后单击“获取设备信息”。

步骤3 （可选）如果提示登录设备，请在“登录”对话框填写登录设备的用户名和密码，单击“确定”。

步骤4 在“网络终端”页签下，选择“主门口机”，配置主门口名称、IP 地址、用户名和密码，选择“启用状态”。

步骤5 单击“保存”。

图4-18 网络终端

步骤6 （可选）将配置应用到其他设备。

1. 单击“应用到...”，在设备导航树选择需要应用该配置的设备，单击“配置”。配置应用到设备。若应用成功，设备右侧显示✓；若失败，显示⚠。单击✓或⚠可查看详细信息。
2. 单击“返回”，返回到配置界面。

4.5.3.2.3 修改用户密码

步骤1 在菜单栏单击 设备配置。

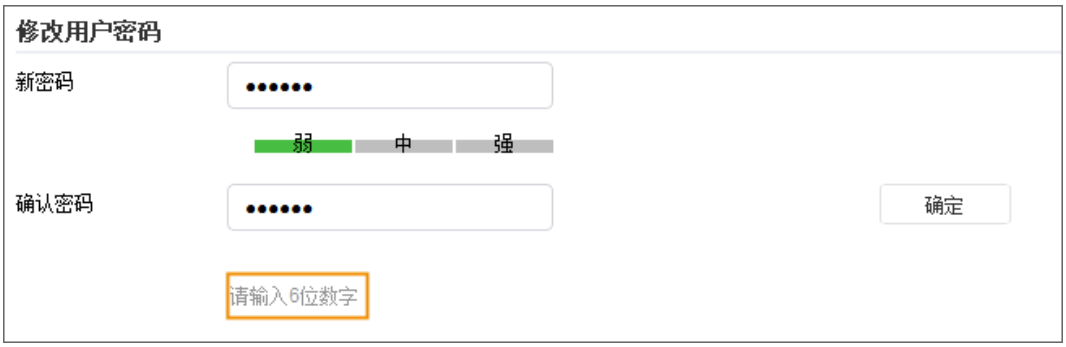
步骤2 在设备列表双击 VTH 设备或单击要配置的 VTH 设备，然后单击“获取设备信息”。

步骤3 （可选）如果提示登录设备，请在“登录”对话框填写登录设备的用户名和密码，单击“确定”。

步骤4 在“密码”页签下，修改信息。

步骤5 单击“确定”。

图4-19 修改用户密码



步骤6 （可选）将配置应用到其他设备。

1. 单击“应用到...”，在设备导航树选择需要应用该配置的设备，单击“配置”。配置应用到设备。若应用成功，设备右侧显示✓；若失败，显示⚠。单击✓或⚠可查看详细信息。
2. 单击“返回”，返回到配置界面。

4.5.3.2.4 报警设置

步骤1 在菜单栏单击

。

步骤2 在设备列表双击 VTH 设备或单击要配置的 VTH 设备，然后单击“获取设备信息”。

步骤3 （可选）如果提示登录设备，请在“登录”对话框填写登录设备的用户名和密码，单击“确定”。

步骤4 在“报警设置”页签下，配置报警参数。

步骤5 单击“确定”。

图4-20 报警设置

表4-9 报警设置参数

参数	说明
区	区号。

参数	说明
类型	选择“红外”、“煤气”、“烟感”、“紧急按钮”、“门磁”、“盗警”、“周界”、“门铃”。的报警类型。
常开/闭	选择“常开”或“常闭”。
状态	选择“瞬时报警”、“延时报警”、“旁路”、“移除”。
进入延时	状态选择“延时报警”，选择进入延时的时长。
退出延时	状态选择“延时报警”，选择退出延时的时长。

步骤6　（可选）将配置应用到其他设备。

1. 单击“应用到...”，在设备导航树选择需要应用该配置的设备，单击“配置”。
   配置应用到设备。若应用成功，设备右侧显示✓；若失败，显示⚠。单击✓或⚠可查看详细信息。
2. 单击“返回”，返回到配置界面。

4.5.3.2.5 模式设置

步骤1　在菜单栏单击

。

步骤2　在设备列表双击 VTH 设备或单击要配置的 VTH 设备，然后单击“获取设备信息”。

步骤3　（可选）如果提示登录设备，请在“登录”对话框填写登录设备的用户名和密码，单击“确定”。

步骤4　在“模式设置”页签下，配置模式参数，单击“确定”。

根据自身模式状态，不同模式下开启或关闭有线防区。

图4-21 模式设置

步骤5　（可选）将配置应用到其他设备。

1. 单击“应用到...”，在设备导航树选择需要应用该配置的设备，单击“配置”。
   配置应用到设备。若应用成功，设备右侧显示✓；若失败，显示⚠。单击✓或⚠可查看详细信息。
2. 单击“返回”，返回到配置界面。

4.5.3.2.6 布防

设置不同布防模式的布防密码。

步骤1　在菜单栏单击

。

步骤2　在设备列表双击 VTH 设备或单击要配置的 VTH 设备，然后单击“获取设备信息”。

步骤3　（可选）如果提示登录设备，请在“登录”对话框填写登录设备的用户名和密码，单击“确定”。

步骤4　在“布防”页签下，选择布防模式，输入布防密码。单击“确定”。

图4-22 布防

说明

布防密码为 6 位数字。

步骤5　（可选）将配置应用到其他设备。

1. 单击“应用到...”，在设备导航树选择需要应用该配置的设备，单击“配置”。配置应用到设备。若应用成功，设备右侧显示✓；若失败，显示⚠。单击✓或⚠可查看详细信息。
2. 单击“返回”，返回到配置界面。

4.5.3.2.7 撤防

填写撤防操作需输入的撤防密码。

步骤1　在菜单栏单击

。

步骤2　在设备列表双击 VTH 设备或单击要配置的 VTH 设备，然后单击“获取设备信息”。

步骤3　（可选）如果提示登录设备，请在“登录”对话框填写登录设备的用户名和密码，单击“确定”。

步骤4　在“撤防”页签下，输入撤防密码。

步骤5　单击“确定”。

图4-23 撤防

说明

撤防密码为 6 位数字。

步骤6　（可选）将配置应用到其他设备。

1. 单击“应用到...”，在设备导航树选择需要应用该配置的设备，单击“配置”。配置应用到设备。若应用成功，设备右侧显示✓；若失败，显示⚠。单击✓或⚠可查看详细信息。
2. 单击“返回”，返回到配置界面。

4.5.3.2.8 预留信息

预留您的信息便于密码重置操作。

步骤1　在菜单栏单击 设备配置。

步骤2　在设备列表双击 VTH 设备或单击要配置的 VTH 设备，然后单击“获取设备信息”。

步骤3　（可选）如果提示登录设备，请在“登录”对话框填写登录设备的用户名和密码，单击“确定”。

步骤4　在“预留信息”页签下，配置预留信息。

步骤5　填写您的手机号码。

步骤6　单击“保存”。

图4-24 预留信息

步骤7　（可选）将配置应用到其他设备。

1. 单击“应用到...”，在设备导航树选择需要应用该配置的设备，单击“配置”。配置应用到设备。若应用成功，设备右侧显示✓；若失败，显示⚠。单击✓或⚠可查看详细信息。
2. 单击“返回”，返回到配置界面。

4.5.3.2.9 IPC 信息

步骤1　在菜单栏单击 设备配置。

步骤2　在设备列表双击 VTH 设备或单击要配置的 VTH 设备，然后单击“获取设备信息”。

步骤3　（可选）如果提示登录设备，请在“登录”对话框填写登录设备的用户名和密码，单击“确定”。

步骤4　在“IPC 信息”页签下，在下拉列表中选择要配置的 IPC 编号。

步骤5　配置 IPC 名称、IP 地址、用户名、IPC 密码，单击“保存”。

图4-25 IPC 信息

表4-10 配置 IPC 参数

参数	参数说明
IPC 名称	设置 IPC 的名称。
IPC IP	填写需要修改的 IP 地址。
IPC 用户名	填写 IPC 登录用户名。

参数	参数说明
码流类型	选择“主码流”或“辅码流”。根据实际场景选择适合的码流。
IPC 端口	IPC 的端口号。
IPC 密码	填写 IPC 登录密码。

步骤6　（可选）将配置应用到其他设备。

1. 单击“应用到...”，在设备导航树选择需要应用该配置的设备，单击“配置”。配置应用到设备。若应用成功，设备右侧显示✓；若失败，显示⚠。单击✓或⚠可查看详细信息。
2. 单击“返回”，返回到配置界面。

4.5.3.3 VTS

步骤1　在菜单栏单击

。

步骤2　在设备列表双击 VTS 设备或单击要配置的 VTS 设备，然后单击“获取设备信息”。

步骤3　（可选）如果提示登录设备，请在“登录”对话框填写登录设备的用户名和密码，单击“确定”。

步骤4　配置 VTS 设备参数。

步骤5　单击“保存”。

图4-26 配置 VTS 设备参数

表4-11 SIP 服务器信息

参数	说明
服务器地址	SIP 服务器 IP 地址
SIP 服务器域名	SIP 服务器域名。

参数	说明
服务器端口	SIP 服务器端口。
使能	选择“使能”。

表4-12 新增门口机

参数	说明
新增门口机	单击“新增门口机”，新增门口机。
门口机编号	添加的门口机编号。
类型	选择“单元门口机”或“围墙机”
门口机名字	VTS 门口机名称。
门口机 IP	VTS 门口机 IP 地址。
用户名	VTS 门口机登录用户名。
密码	VTS 门口机登录密码。
中号	VTS 门口机中号信息。
使能	选择“使能”。

4.5.4 安卓广告机设备

支持批量配置安卓广告机设备的 APP 的 IP 地址、Android 调试，以及导出设备日志到本地。

4.5.4.1 APP 配置

支持批量修改 APP 注册时的 IP 地址。

步骤1 在菜单栏单击

。

步骤2 在设备列表双击要配置的安卓广告机设备或单击要配置的安卓广告机设备，然后单击“获取设备信息”。

步骤3 （可选）如果提示登录设备，请在“登录”对话框填写登录设备的用户名和密码，单击“确定”。

步骤4 在“APP 配置”页签下，填写 APP 注册的 IP 地址信息。单击“修改”。

步骤5 （可选）将配置应用到其他设备。

1. 单击“应用到...”，在设备导航树选择需要应用该配置的设备，单击“配置”。配置应用到设备。若应用成功，设备右侧显示✓；若失败，显示⚠。单击✓或⚠可查看详细信息。
2. 单击“返回”，返回到配置界面。

图4-27 APP 配置

4.5.4.2 Android 调试

配置 Android 调试开关。

步骤1　在菜单栏单击

。

步骤2　在设备列表双击要配置的安卓广告机设备或单击要配置的安卓广告机设备，然后单击“获取设备信息”。

步骤3　（可选）如果提示登录设备，请在“登录”对话框填写登录设备的用户名和密码，单击“确定”。

步骤4　在“Android 调试”页签下，选择“开”。单击“调试”。

步骤5　（可选）将配置应用到其他设备。

1. 单击“应用到...”，在设备导航树选择需要应用该配置的设备，单击“配置”。配置应用到设备。若应用成功，设备右侧显示✓；若失败，显示⚠。单击✓或⚠可查看详细信息。
2. 单击“返回”，返回到配置界面。

图4-28 Android 调试

4.5.4.3 导出日志

导出安卓广告机设备日志到本地。

步骤1　在菜单栏单击

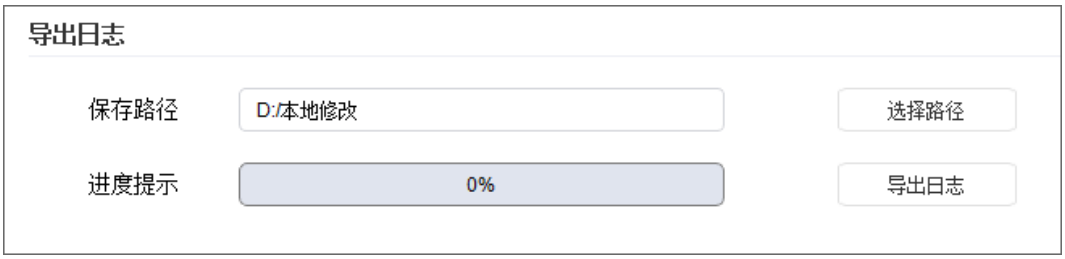
。

步骤2　在设备列表双击要配置的安卓广告机设备或单击要配置的安卓广告机设备，然后单击“获取设备信息”。

步骤3　（可选）如果提示登录设备，请在“登录”对话框填写登录设备的用户名和密码，单击“确定”。

步骤4　在“导出日志”页签下，单击“选择路径”，选择要导出的文件夹。单击“导出日志”。进度提示导出日志速度的百分比。

图4-29 导出日志



4.6 配置系统信息

4.6.1 校准设备时间

在实行夏令时的国家或者地区使用设备时，需要执行此步骤。

步骤1　在菜单栏单击

，单击“校时”页签。

步骤2　在设备导航树选择需要校准的单台或者多台设备。

步骤3　根据实际情况选择设备同步时间的方式。

- 在“时间同步”区域单击“手动同步”，同步设备时间为设置的时间。
- 在“时间同步”区域单击“同步 PC”，以 PC 时间为基准调整设备时间。
- 在“时区”区域选择“NTP 设置”，设置 NTP 服务器参数，参数说明请参见表 4-13。

步骤4　（可选）选择“启用夏令时”，设置夏令时参数。

步骤5　单击“保存”。

图4-30 设置时间

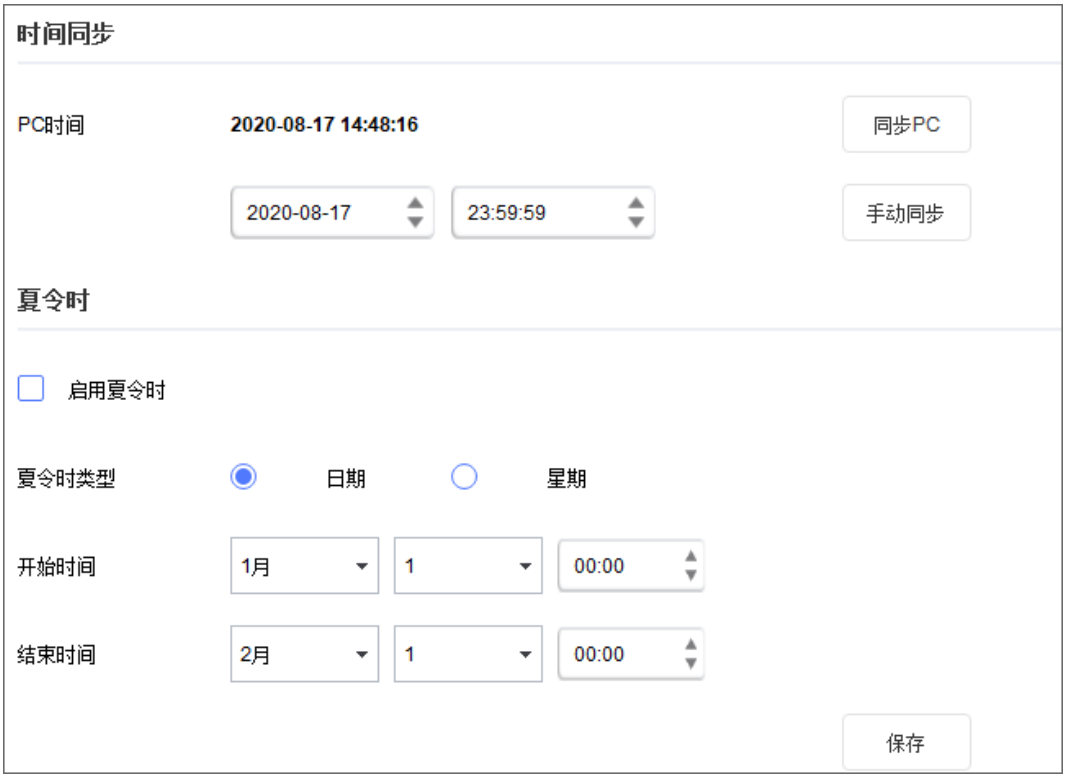


图4-31 NTP 设置

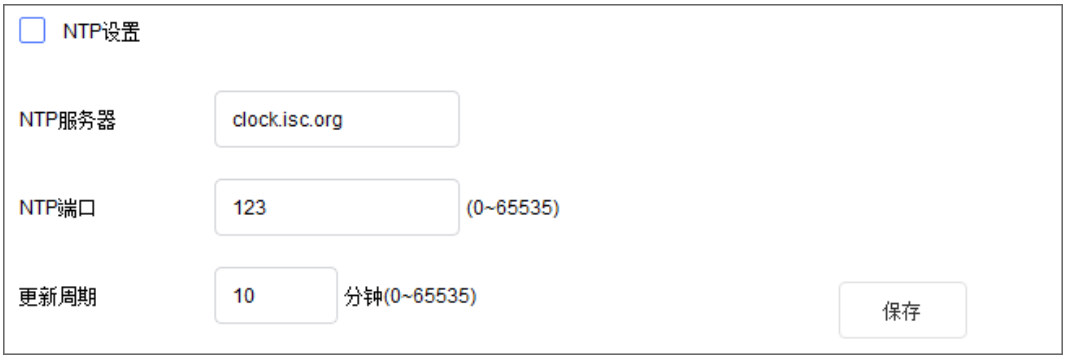


表4-13 NTP 参数说明

参数	说明
NTP 服务器	设置为对接 NTP 服务器的 IP 地址或者域名。
NTP 端口	设置为对接 NTP 服务器的端口。
更新周期	设备向 NTP 服务器同步时间的间隔时间。

表4-14 夏令时参数说明

参数	说明
夏令时类型	根据实际情况选择类型为“日期”或者“星期”。

参数	说明
开始时间	设置夏令时的开始时间和结束时间。
结束时间	

4.6.2 重启设备

自动重启或者手动重启设备。

注意

重启会造成业务中断，请尽量选择业务量小的时间重启设备。

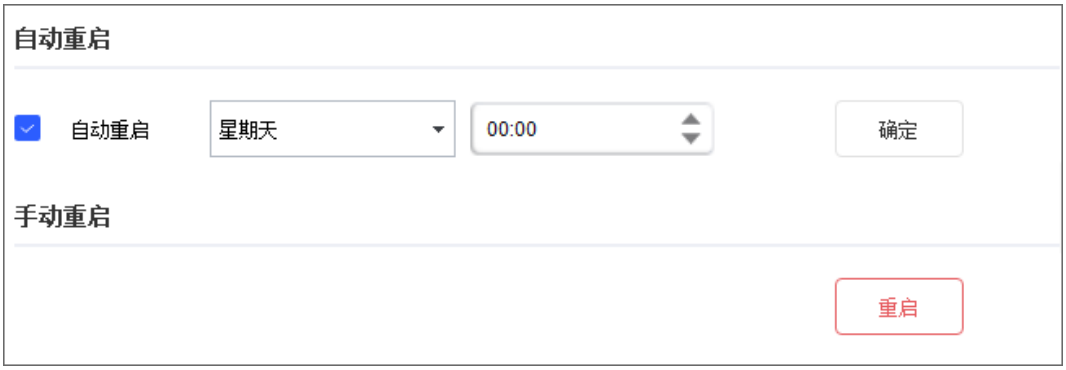
步骤1　在菜单栏单击 系统配置。

步骤2　在设备导航树选择需要重启的单台或者多台设备。

步骤3　根据实际情况选择设备的重启方式。

- 若要“自动重启”，选择“自动重启”，设置重启星期和时间，单击“确定”，设备在对应时间自动重启。
- 若要“手动重启”，单击“重启”，设备立即重启。

图4-32 重启设备



4.6.3 恢复设置

4.6.3.1 恢复默认

通过“恢复默认”，除如下信息以外，其他信息均会恢复为默认设置。

- 设备 IP 地址等网络参数。
- 所有用户信息（包括 admin 的密码、添加的用户等）。

步骤1　在菜单栏单击 系统配置。

步骤2　在设备导航树选择需要恢复默认的单台或者多台设备。

步骤3　单击“恢复”页签。

步骤4　单击“恢复默认”，然后单击“确定”，开始恢复设备的默认设置。

若恢复默认成功，设备右侧显示✓；若失败，显示⚠。单击✓或⚠可查看详细信息。

图4-33 恢复设备默认设置

4.6.3.2 恢复出厂

通过“恢复出厂”，设备所有参数（包括设备 IP 地址等网络参数）均会恢复到默认设置。

步骤1 在菜单栏单击 系统配置。

步骤2 在设备导航树选择需要恢复出厂的单台或者多台设备。

步骤3 单击“恢复”页签。

步骤4 单击“恢复出厂”，根据提示单击“确定”，开始恢复设备的出厂设置。

若恢复出厂成功，设备右侧显示✓；若失败，显示⚠。单击✓或⚠图标可查看详细信息。

图4-34 恢复设备出厂设置

4.6.3.3 导出设备配置到本地

步骤1 在菜单栏单击 系统配置，单击“恢复”页签。

步骤2 在设备导航树选择需要导出信息的单台或者多台设备。

步骤3 单击“导出”，在弹出的窗口选择保存位置，填写文件名称，单击“保存”。

若导出成功，设备右侧显示✓；若失败，显示⚠。单击✓或⚠可查看详细信息。

图4-35 导出设备配置到本地

4.6.3.4 复制其他设备的配置

同一类型、型号和软件版本的设备，支持配置复用，即完成一台设备配置后，与该设备相同类型、型号和软件版本的其他设备，通过导入配置，可以一次性应用相同的配置，而无需一一重新配置。

前提条件

已准备配置文件。

操作步骤

步骤1　在菜单栏单击 系统配置，单击“恢复”页签。

步骤2　在设备导航树选择单台或者多台设备。

步骤3　单击“导入”，根据界面提示导入配置信息，该配置信息将应用到选择的设备中与配置信息所属设备相同类型、型号和软件版本的设备上。

若导入成功，设备右侧显示✓；若失败，显示⚠。单击✓或⚠可查看详细信息。

图4-36 导入配置到设备

4.6.4 修改设备密码

步骤1　在菜单栏单击 系统配置。

步骤2　在设备导航树选择单台或者多台设备。

说明

选择的多台设备的登录密码必须相同。

步骤3　单击“密码”页签。

步骤4　填写设备旧密码，单击“校验”。

如果设备旧密码填写正确，即可设置新密码，否则无法设置新密码，请确保旧密码填写正确。

步骤5　设置新密码。

请根据密码强弱提示设置高安全性密码。

步骤6　单击“确定”。

图4-37 修改设备密码

说明

新密码可设置为 6 位纯数字，或 8 位～32 位必须由数字、字母和特殊字符（除“'”、“"”、“;”、“:”、“&”外）三种类型中的至少两种组成。请根据密码强弱提示设置高安全性密码。

4.6.5 视频配置

用于设置设备上视频的视频制式。

步骤1　在菜单栏单击 系统配置，单击“批量”页签。

步骤2　在设备导航树选择要设置视频制式的设备，在“视频制式”下拉列表选择视频制式，单击“保存”。

若视频制式设置成功，设备右侧显示✓；若失败，显示⚠。单击✓或⚠可查看详细信息。

图4-38 设置视频制式

4.6.6 批量表单操作

用于批量配置表单操作。

步骤1　在菜单栏单击 系统配置，单击“批量”页签。

步骤2　在设备导航树选择要设置视频制式的设备，在“视频制式”下拉列表选择视频制式，单击“保存”。

若视频制式设置成功，设备右侧显示✓；若失败，显示⚠。单击✓或⚠可查看详细信息。

步骤3　选择“操作类型”。单击“打开”，填写模板信息。单击“配置”。

图4-39 批量配置表单操作

表4-15 操作类型参数说明

参数	说明
批量修改 IP	批量修改表格内的 IP 地址。
生成登录密码	批量生成登录密码。
修改密码	批量修改登录用户密码。
批量升级	批量升级设备。
允许清单追加	批量配置 IP 地址允许访问设备。

参数	说明
禁用清单追加	批量配置 IP 地址禁止访问设备。
编码配置	批量配置编码参数。 **说明** 仅支持配置 h264 或 h265，支持设置码流，支持智能编码开启和关闭。

4.6.7 产品授权

4.6.7.1 更新设备 License

当设备 License 出现问题后，需要更新 License。本方式需要联系技术支持人员通过申请 License 电子流申请 License。通过本方式申请的 License 有效期，取决于审批有效期。

步骤1　在菜单栏单击

，选择“授权 > 通用”。

步骤2　在设备导航树选择需要授权的单台或者多台设备。。

步骤3　单击“导出配置”，导出设备配置信息到本地。

若导出配置成功，设备右侧显示✓；若导出配置失败，设备右侧显示⚠。单击✓或⚠查看详细信息。

步骤4　联系对接的技术支持人员获取 License。

说明

License 需要绑定设备配置信息。联系技术支持人员时，请提供设备配置信息。

步骤5　导入 License 到设备。

1. 单击“选择 License”，选择申请的 License。
2. 单击“导入 License”，将 License 导入设备。

图4-40 更新设备 License

4.6.7.2 一键授予设备 License

当公司研发人员需要临时授予设备 License，可以采用本方式。本方式直接授予设备 License，而无需使用电子流申请 License，授予的 License 有效期为 30 天。

注意事项

- 仅公司员工具有本操作权限。
- 在公司内网操作。
- 授权内容为所填写的料号的配置。

操作步骤

步骤1　在菜单栏单击 系统配置，选择“授权 > 研发”。

步骤2　（可选）如果未登录，请登录。单击“登录”，在弹出的对话框填写员工工号和密码，单击“确定”。

步骤3　在设备导航树选择需要授权的单台或者多台设备。

步骤4　填写设备料号(P/N)，单击“一键授权”。

若一键授权成功，设备右侧显示✓；若一键授权失败，显示⚠。单击✓或⚠查看详细信息。

图4-41 一键授权

4.6.7.3 一键恢复设备 License 为出厂状态

当设备出现问题需要维修时，为确保顺利维修，建议维修之前先恢复设备 License 为出厂状态。

注意事项

- 仅公司员工具有本操作权限。
- 在公司内网操作。
- 设备必须在产线生产过。
- 设备必须有序列号（S/N）和整机料号，且必须和产线生产时所设置的一致。

操作步骤

步骤1　在菜单栏单击 系统配置，选择“授权 > 维修”。

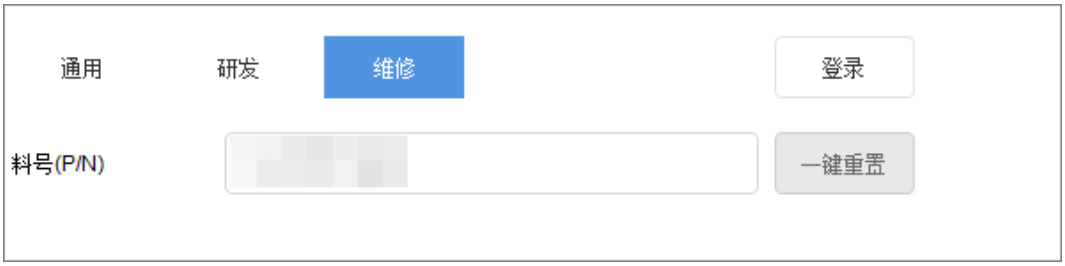
步骤2　（可选）如果未登录，请登录。单击“登录”，在弹出的对话框填写员工工号和密码，单击“确定”。

步骤3　在设备导航树选择需要授权的单台或者多台设备。

步骤4　填写设备料号，单击“一键重置”。

将设备 License 重置为出厂状态。若重置成功，设备右侧显示✓；若重置失败，设备右侧显示⚠。单击✓或⚠查看详细信息。

图4-42 一键重置



4.6.8 证书管理

4.6.8.1 国标 35114 简介

《公共安全视频监控联网信息安全技术要求》（GB 35114-2017）已正式发布。该标准规定公共安全领域视频监控联网视频信息以及控制信令信息安全保护的技术要求。标准根据安全保护强弱，将前端设备安全能力分为三个等级，等级和等级具有的能力请参见表 4-16。当前大部分设备只支持 A 级标准。

说明

- 设备指 IPC、球机、NVR 等编码设备。
- 下文出现的国标 35114 协议，都指国标 35114 协议 A 级。

表4-16 等级与能力

等级	基于数字证书与管理平台双向设备认证能力、用户双向设备认证能力、控制信令校验等能力	基于数字证书的视频数据签名能力	视频加密能力
A	√	-	-
B	√	√	-
C	√	√	√

4.6.8.2 配置流程

采用国标 35114 协议组网，组网中设备完成基础配置后，需要执行图 4-43 所示流程开启国标 35114 协议。配置流程说明请参见表 4-17。

图4-43 国标 35114 配置流程

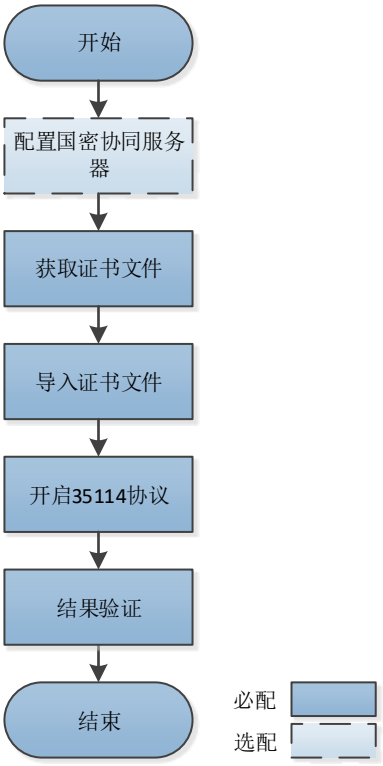


表4-17 配置流程说明

流程	说明
配置国密协同服务器	选配项。安全模块形态包括芯片、TF 卡和软件（国密协同服务器）。如果采用前两种形态，无需配置该项。安全模块含有密码算法、安全功能，实现秘钥管理机制。
获取证书文件	证书文件包括设备身份证书、CA 证书和用户证书。如果有吊销证书需要获取吊销列表文件。
导入证书文件	将获取的证书文件导入到各设备中，用于验证对端设备或接入用户身份是否合法。
开启 35114 协议	启用 35114 协议，组网设备之间采用 35114 协议交互。
结果验证	确认配置的 35114 协议可用。

4.6.8.3 开启 35114 协议

启用 35114 协议，确认设备间采用 35114 协议交互。

步骤1　在菜单栏单击

，单击“证书管理”页签。

步骤2　在设备导航树选择需要导入配置文件的设备。

步骤3　准备配置文件。在“GB28181 配置”区域单击“下载模板”，根据组网情况填写模板，并保存。

说明

表中出现的服务器 X，X 代表数字 1 或 2。如果配置两个 SIP 服务器则服务器 1 和服务器 2 都要配置

表4-18 参数说明

参数	说明
IP	待配置 35114 协议的设备 IP。
接入总使能	设置为 TRUE，确认开启协议总开关。
服务器 X-平台接入使能	设置为 2，确认开启 35114 协议。
服务器 X-编号	SIP 服务器编号，默认为 34020000002000000001。 例如：IPC 对接 NVR，NVR 作为 IPC 的 SIP 服务器，则此处填写为 NVR 的编号。下文提及的 SIP 服务器都是相同的概念。
服务器 X-域	SIP 服务器域名编号，默认为 3402000000
服务器 X-IP	SIP 服务器 IP。
服务器 X-设备编号	作为 SIP 服务器的设备为接入设备分配的编号，每台设备的编号是唯一的，默认为 34020000001320000001。
服务器 X-密码	默认为 12345678。
服务器 X-本地端口	默认为 5060。
服务器 X-服务器端口	SIP 服务器端口，默认为 5060。
服务器 X-注册有效期	注册后的有效时长，默认为 3600，单位：秒。
服务器 X-注册间隔	两次注册之间的时间间隔，默认为 60，单位：秒。
服务器 X-心跳周期	设备与 SIP 服务器之间保活时间，默认为 60。
服务器 X-最大心跳超时次数	统计设备与 SIP 服务器在超过心跳时间的次数，一旦超过此次数，即设备主动断开与 SIP 服务器之间的通讯。默认为 3 次。
服务器 X-行政区划代码	默认为 6532。
接服务器 X-入模块识别码	设备以何种方式与 SIP 服务器进行通讯，一般为设备端与服务器端约定好的值，默认为 00000101。
服务器 X-通道 ID	设置通道号，默认为 34020000001310000001。
服务器 X-报警级别	设置报警级别，默认为 1。
服务器 X-报警通道 ID	设置报警通道号，默认为 34020000001310000001。
服务器 X-报警级别	设置报警级别，默认为 1。
服务器 X-报警通道 ID	设置报警通道号，默认为 34020000001310000001。
服务器 X-音频输出通道 ID	设置报警通道号，默认为 34020000001310000001。

步骤4　在“GB28181 配置”区域，单击“打开”，根据提示选择制作的模板文件，单击“导入”。

图4-44 启用 35114 协议

4.6.8.4 导入证书到设备

4.6.8.4.1 获取证书文件

以离线的方式通过 PKCS#10 标准证书请求文件向证书颁发机构申请本地设备身份证书，并获取 CA 证书、CRL 吊销列表；向对端接入设备管理者获取对端设备身份证书；向设备管理员获取用户证书。

在线颁发数字证书的情形下设备会自动连接证书颁发机构服务器获取证书，无需用到工具。

本地身份证书

通过工具从设备端导出本地设备证书请求到本地，通过证书请求发送到证书颁发机构，申请本地设备身份证书。

步骤1　在菜单栏单击

，单击“证书管理”页签。

步骤2　在设备导航树选择一台或多台设备。

步骤3　在“导出证书请求”区域选择网络类型。

- 公安信息网：公安机关因工作需要，专门设立的网络。
- 视频专网：为了保证网络带宽和视频的流畅性，建立的视频专用网络。

步骤4　单击“打开”，指定证书请求保存路径。

步骤5　单击“导出”，导出证书请求到指定保存路径。

步骤6　将证书请求发送到用户指定的证书颁发机构，申请本地设备身份证书。

图4-45 导出证书请求

远端身份证书

向对端接入设备管理者获取对端设备身份证书。

CA 证书和 CRL 吊销列表

一般情况下申请本地设备身份证书时，证书机构返回身份证书时，同时反馈 CA 证书和 CRL 吊销列表。如果没有反馈请在证书机构网站下载。

用户证书

根据国标 35114 规定，为 WEB 用户提供 U 盾登录方式，校验用户身份。联系设备管理员获取用户证书。用户证书的申请与制作方法，请参见 35114 解决方案的部署指南。

4.6.8.4.2 导入证书文件

将证书文件导入到设备，用于双向身份认证。

步骤1　在菜单栏单击 系统配置，单击“证书”页签。

步骤2　在设备导航树选择一台或多台设备。

步骤3　按照顺序，导入 CA 证书、本地身份证书、远端身份证书、用户证书、CRL 吊销列表。

1. 单击“打开，选择证书。
   - ◇ 本地身份证书选择证书存放的文件夹，导入时设备自动匹配序列号，导入正确的证书文件。
   - ◇ 远端身份证书选择证书时按【Ctrl】键，支持选择多个证书文件。
   - ◇ CA 证书请根据证书机构提供导入。如果 CA 证书有多级，先导入根 CA 证书再导入子 CA 证书。如果本地证书、远端证书、用户证书由不同的 CA 机构签发，多个机构的 CA 证书都需要导入。
2. 单击“导入”，导入证书。
   若成功导入证书，设备右侧显示✓；若失败，显示⚠。单击✓或⚠查看详细信息。

4.6.8.5 （可选）配置国密协同服务器

安全模块采用软件（国密协同服务器）形态时需要配置。国密协同服务器含有密码算法、安全功能，实现密钥管理机制。配置国密协同服务器后，才可以导出设备的证书请求文件用于申请设备身份证书。安全模块采用芯片或 TF 卡等硬件密码模块，忽略此章节。

前提条件

已部署国密协同服务器，并且已获取国密协同服务器的 IP 地址、端口号。

操作步骤

步骤1　在菜单栏单击 系统配置，单击“证书”页签。

步骤2　在设备列表选择需要配置国密协同服务器的设备，支持选择多个。

步骤3　在“国密协同服务器”区域填写国密协同服务器的 IP 地址和端口号。

步骤4　单击“保存”。

图4-46 配置国密协同服务器

4.6.8.6 结果验证

详细介绍请参见“附录 1 验证 35114 协议”。

4.7 重置密码

重置设备管理员 admin 的登录密码。

说明

- 工具仅支持重置与工具所在 PC 同一网段的设备的密码，且仅支持重置设备的管理员 admin 的密码。如果需要重置设备其他用户的密码，需要使用管理员账号登录设备，来修改其他用户的密码。
- 仅支持重置已初始化的设备的密码。
- 不同设备支持密码重置的能力可能不一样，部分设备不支持密码重置。设备列表中设备置灰表示该设备不支持密码重置。

4.7.1 批量重置

适用于同时重置两台或两台以上设备登录密码的情形。使用该方式，仅支持通过发送 XML 文件重置设备登录密码。

步骤1　在菜单栏单击

。

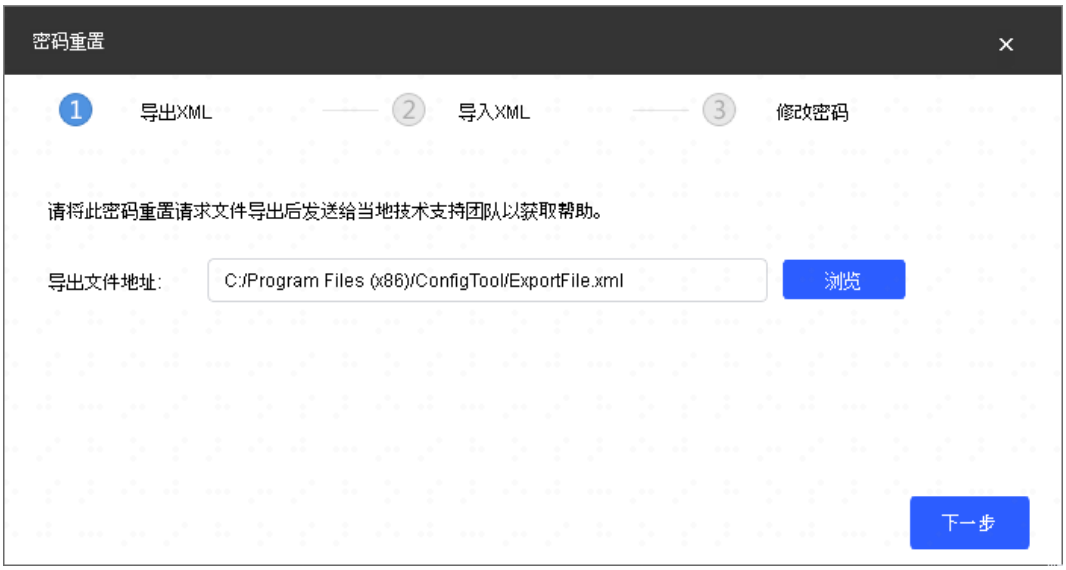
步骤2　在设备列表选择需要重置密码的设备，单击“批量重置”，在弹出的对话框单击“确定”。

步骤3　导出 ExportFile.xml 文件。

1. 单击“浏览”，在弹出的对话框选择 ExportFile.xml 文件的保存路径，单击“选择”。
2. 单击“下一步”，根据提示操作，完成 ExportFile.xml 导出。

步骤4　使用通过设备厂商官方认证的企业邮箱将导出的 ExportFile.xml 文件发送给当地的技术支持团队，并从此团队获取 result.xml 文件。

图4-47 导出 ExportFile.xml



步骤5　导入 result.xml。单击“打开”，从保存路径导入 result.xml 文件，单击“下一步”。导入 XML 文件成功后，自动进入修改密码界面。

说明

若导入 XML 的窗口已关闭，在“密码重置”界面左上方单击“导入 Result.xml”，在弹出的对话框导入 result.xml 文件。

图4-48 导入 result.xml

步骤6 修改密码。

输入“新密码”和“确认密码”。

步骤7 单击“完成”，工具开始重置设备密码。

若重置成功，设备右侧显示✓；若重置失败，设备右侧显示⚠。单击✓或⚠查看详细信息。

说明

设备不同，密码长度不同。新密码可设置为 6 位纯数字，或 8 位～32 位必须由数字、字母和特殊字符（除“'”、“"”、“;”、“:”、“&”外）三种类型中的至少两种组成。请根据密码强弱提示设置高安全性密码。

图4-49 重置密码

4.7.2 单台重置

重置单台设备登录密码。

说明

设备不同重置密码方式可能不同，请以实际界面为准，本文以重置一款设备的登录密码为例。

步骤1　在菜单栏单击 密码重置。

步骤2　在设备列表选择需要密码重置的设备，单击“密码重置”。

步骤3　重置密码。设备支持的密码重置方式以界面显示为准。

- 通过扫描二维码重置密码。
  1. 选择“重置方式”为“二维码”。
  2. 按照提示获取并填写安全码。
  3. 设置新密码。
- 通过发送 XML 文件重置密码，详细介绍请参见“4.7.1 批量重置”。

说明

新密码可设置为 6 位纯数字，或 8 位～32 位必须由数字、字母和特殊字符（除“'”、“"”、“;”、“:”、“&”外）三种类型中的至少两种组成。请根据密码强弱提示设置高安全性密码。

步骤4　单击“确定”，开始重置设备登录密码。

若重置成功，设备右侧显示✓；若重置失败，设备右侧显示⚠。单击✓或⚠查看详细信息。

图4-50 重置密码

4.8 楼宇配置

通过模板填写 VTO/VTH 设备详细信息，将设备信息导入到快速配置工具。配置信息

说明

不同设备的编码参数可能不同，请以实际界面显示为准。

步骤1　在菜单栏单击 楼宇配置。

步骤2　单击“打开模板”，填写配置参数。

步骤3　单击“导入”，导入配置好的表格信息。

步骤4　选择设备，单击“匹配”，配置表格中填好的设备信息。

图4-51 楼宇批量配置

表4-19 楼宇配置参数

参数		说明
设备类型		选择“围墙机”、“单元门口机”、“室内机”、“二次确认机”不同设备类型。
设备名称		设备的名称。
设备 ID		设备的 SN 号。
网络信息	IP 地址	设备的 IP 地址。
	子网	设备的子网掩码。
	网关	设备的网关。
	端口	设备的端口。
登录信息	用户名	IP 地址的登录名。
	登录密码	IP 地址的登录密码。
物理信息	区号	区号。
	幢号	楼宇设备所在幢号。
	单元号	楼宇设备所在单元号。
	房间号	楼宇设备所在房间号。

参数		说明
	分机号	楼宇设备所在分机号。
	中心号码	楼宇设备的中心号码。
	主 VTO	设置主 VTO 号。
SIP 服务器信息	服务器 IP	SIP 服务器 IP 地址。
	注册密码	SIP 服务器注册密码。
	SIP 端口	SIP 服务器的端口号。
	SIP 用户名	SIP 服务器用户名。
	SIP 密码	SIP 服务器登录密码。
	服务器类型	选择“VTO”、“VTNS”、“Private”、“/”服务器类型。
	SIP 域	SIP 服务器域名。
居住信息	姓	居住者的“姓”。
	名	居住者的“名”。

4.9 CGI 协议

支持 CGI 批量配置信息或通过表单配置设备信息。

说明

配置信息时，CGI 命令使用 https 协议传输。否则会出现“不安全...”的信息提示。

4.9.1 通过 CGI 配置信息

步骤1　在菜单栏单击 CGI协议。

步骤2　（可选）如果待修改设备通过模板添加或通过搜索添加，请检查“搜索设置”对话框，确保在该对话框填写正确的设备用户名和密码。

步骤3　填写 Url 路径，Url 路径确定无误后，单击“配置”。

图4-52 通过 CGI 配置信息

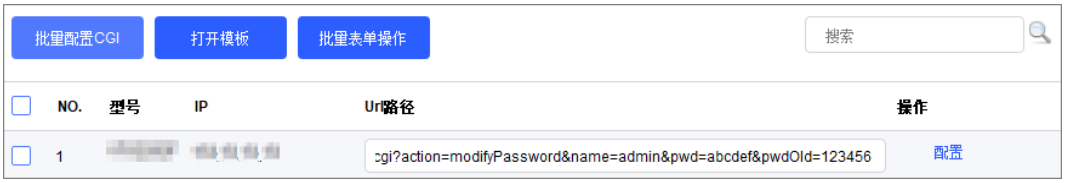


表4-20 表单参数说明

参数	说明
IP 地址	设备 IP 地址。
端口号	设备端口号。
用户名	设备登录用户名。
密码	设备登录密码。
CGI 配置命令	设备的 CGI 配置命令路径。
协议类型（0-http,1-https）	CGI 协议类型。 ● http：超文本传输协议，信息是明文传输。且连接简单，无状态。 ● https：具有安全性的加密传输协议，确保数据传输的安全。

参数	说明
设置结果	针对下发的 CGI 命令执行的结果。提示成功，设置成功；提示失败，设置失败。

4.9.2 通过 CGI 批量配置信息

步骤1　在菜单栏单击

。

步骤2　（可选）如果待修改设备通过模板添加或通过搜索添加，请检查“搜索设置”对话框，确保在该对话框填写正确的设备用户名和密码。

步骤3　选择需要批量配置 IP 地址，单击“批量配置 CGI”，填写 Url 路径。

步骤4　确保批量选择的设备路径一致，单击“确定”。

图4-53 通过 CGI 批量配置信息

4.9.3 通过表单配置信息

步骤1　在菜单栏单击

。

步骤2　（可选）如果待修改设备通过模板添加或通过搜索添加，请检查“搜索设置”对话框，确保在该对话框填写正确的设备用户名和密码。

步骤3　单击“打开模板”，填写 IP 地址、端口号、用户名、密码、CGI 配置命令等信息。编辑完成后，保存并关闭模板。

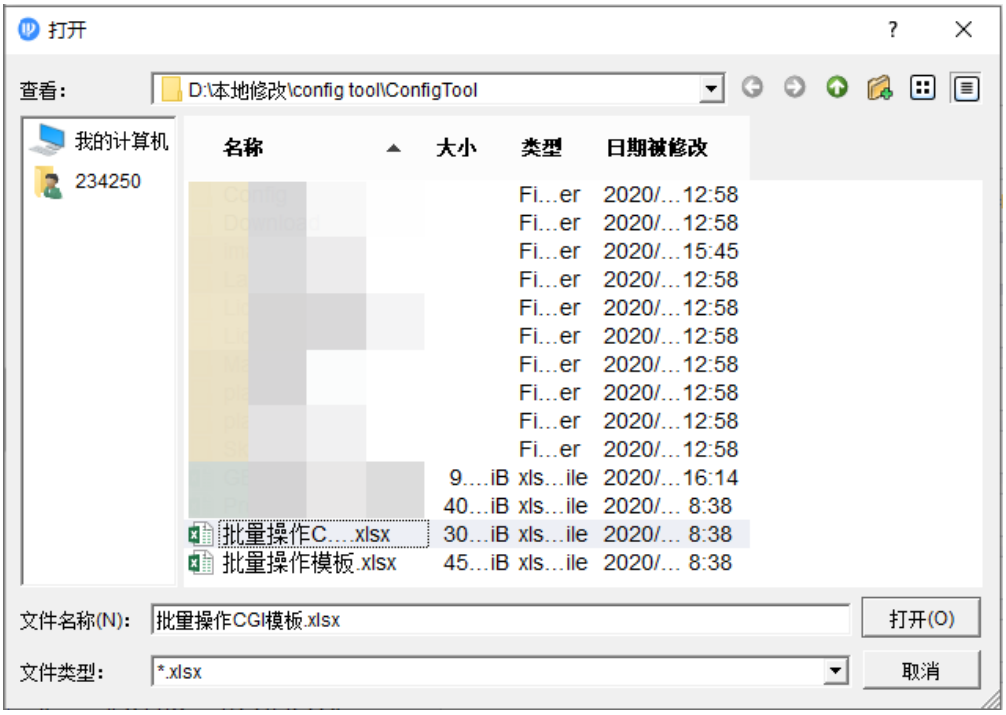
图4-54 通过表单配置信息

IP地址	端口	用户名	密码	CGI配置命令	协议类型(0 - http, 1 - https)	设置结果
[illegible]		admin	admin	/cgi-bin/configManager.cgi?action=setConfig&VideoInDayNight[0][0].Mode=BlackWhite	0	
[illegible]		admin	admin	/cgi-bin/configManager.cgi?action=setConfig&VideoStandard=PAL	0	
[illegible]		admin	admin	/cgi-bin/userManager.cgi?action=modifyPassword&name=admin&pwd=abcdef&pwdOld=12345	1	

步骤4　返回 CGI 协议界面。

步骤5　单击“批量表单操作”，选择“批量操作 CGI 模板” 。单击“打开”，后台自动通过表单配置信息。配置完成后，弹框提示打开模板，确认配置结果。

图4-55 表单批量配置信息



4.10 查看帮助文档

- 单击工具右上角，单击“帮助”，查看工具使用说明书。
- 单击工具右上角，单击“QA”，查看工具的常见问题解答。

4.11 查看工具版本

单击工具右上角，单击“关于”，查看工具版本、开源声明和软件许可协议。

第 5 章 工具配置

配置使用工具登录设备的模式，以及升级设备相关参数，例如升级设备时升级超时时间、网络连接最长时间、升级传输速度等。

步骤1　单击工具右上角，然后单击“设置”。

步骤2　配置登录设备的模式及升级设备相关参数。

步骤3　单击“确定”。

图5-1 工具配置

表5-1 工具配置说明

参数	说明
登录模式	选择登录设备的模式。 ● 安全模式（默认）：登录设备时只使用安全的认证方式。当设备支持安全模式登录时，请选择该模式。 ● 兼容模式：登录设备时会依次尝试安全的认证方式和不安全的认证方式。当设备仅支持兼容模式时，建议升级设备程序，或使用兼容模式。 **注意** 兼容模式存在潜在的安全风险，请谨慎选择。
升级超时时间(/分)	设备升级时，单台设备的最长升级时间。 当设备升级的时间大于设置值时，工具提示升级失败。
网络超时时间(/秒)	设备升级时，网络连接最长时间。 当设备升级时网络连接时间大于设置值，设备停止升级。

参数	说明
升级传输速度（/次）	设备升级包的传输速度。 ● 当 100MB≤升级包容量＜2GB 之间，根据升级时间选择 1KB 或 16KB，设置为 16KB 时，升级速度更快。 ● 当升级包容量＜100MB 时，工具自动按照 1KB 上传升级包，此处配置无效。 ● 当升级包容量≥2GB 时，工具自动按照 16KB 上传升级包，此处配置无效。
输出日志	选择“开启”或“关闭”。

附录1 验证 35114 协议

附录1.1 登录设备

验证采用 U 盾登录方式，完成用户身份校验。

登录 WEB 配置界面

步骤1　将 U 盾接入 PC。

步骤2　打开 PC 浏览器，在地址栏输入设备 IP 地址，按【Enter】键。

本文以球机截图为例，其他设备请以实际界面为准。

步骤3　输入用户名和 PIN 码，单击“登录”。

进入设备 WEB 配置界面。

图5-2 登录界面

登录本地配置界面

说明

不支持本地配置的设备可以忽略此章节。

步骤1　将 U 盾接入设备。

步骤2　在本地配置的登录界面，输入用户名和 PIN 码，单击“确定”，如图 5-3 所示。

进入设备本地配置界面。

本文以 NVR 截图为例，其他设备请以实际界面为准。

图5-3 登录界面

附录1.2 添加远程设备

验证能添加远程设备，本文以在 NVR 上以 GB35114 协议添加 IPC 为例，如果 NVR 上查看远程设备，设备在线，则添加远程设备正常。

附录1.3 实时预览

验证能实时预览，本文以在 NVR 预览 IPC 通道为例，要求能查看实时视频画面。

附录2 法律声明

商标声明

- VGA 是 IBM 公司的商标。
- Windows 标识和 Windows 是微软公司的商标或注册商标。
- 在本文档中可能提及的其他商标或公司的名称，由其各自所有者拥有。

责任声明

- 在适用法律允许的范围内，在任何情况下，本公司都不对因本文档中相关内容及描述的产品而产生任何特殊的、附随的、间接的、继发性的损害进行赔偿，也不对任何利润、数据、商誉、文档丢失或预期节约的损失进行赔偿。
- 本文档中描述的产品均“按照现状”提供，除非适用法律要求，本公司对文档中的所有内容不提供任何明示或暗示的保证，包括但不限于适销性、质量满意度、适合特定目的、不侵犯第三方权利等保证。

隐私保护提醒

您安装了我们的产品，您可能会采集人脸、指纹、车牌、邮箱、电话、GPS 等个人信息。在使用产品过程中，您需要遵守所在地区或国家的隐私保护法律法规要求，保障他人的合法权益。如，提供清晰、可见的标牌，告知相关权利人视频监控区域的存在，并提供相应的联系方式。

关于本文档

- 产品请以实物为准，本文档仅供参考。
- 本公司保留随时维护本文档中任何信息的权利，维护的内容将会在本文档的新版本中加入，恕不另行通知。
- 本文档如有不准确或不详尽的地方，或印刷错误，请以公司最终解释为准。
- 本文档供多个型号产品做参考，每个产品的具体操作不逐一例举，请用户根据实际产品自行对照操作。
- 如不按照本文档中的指导进行操作，因此而造成的任何损失由使用方自行承担。
- 如获取到的 PDF 文档无法打开，请将阅读工具升级到最新版本或使用其他主流阅读工具。

附录3 网络安全建议

保障设备基本网络安全的必须措施：

1. 使用复杂密码

请参考如下建议进行密码设置：

- 长度不小于 8 个字符。
- 至少包含两种字符类型，字符类型包括大小写字母、数字和符号。
- 不包含帐户名称或帐户名称的倒序。
- 不要使用连续字符，如 123、abc 等。
- 不要使用重叠字符，如 111、aaa 等。

2. 及时更新固件和客户端软件

- 按科技行业的标准作业规范，设备的固件需要及时更新至最新版本，以保证设备具有最新的功能和安全性。设备接入公网情况下，建议开启在线升级自动检测功能，便于及时获知厂商发布的固件更新信息。
- 建议您下载和使用最新版本客户端软件。

增强设备网络安全的建议措施：

1. 物理防护

建议您对设备（尤其是存储类设备）进行物理防护，比如将设备放置在专用机房、机柜，并做好门禁权限和钥匙管理，防止未经授权的人员进行破坏硬件、外接设备（例如 U 盘、串口）等物理接触行为。

2. 定期修改密码

建议您定期修改密码，以降低被猜测或破解的风险。

3. 及时设置、更新密码重置信息

设备支持密码重置功能，为了降低该功能被攻击者利用的风险，请您及时设置密码重置相关信息，包含预留手机号/邮箱、密保问题，如有信息变更，请及时修改。设置密保问题时，建议不要使用容易猜测的答案。

4. 开启帐户锁定

出厂默认开启帐户锁定功能，建议您保持开启状态，以保护帐户安全。在攻击者多次密码尝试失败后，其对应帐户及源 IP 将会被锁定。

5. 更改 HTTP 及其他服务默认端口

建议您将 HTTP 及其他服务默认端口更改为 1024～65535 间的任意端口，以减小被攻击者猜测服务端口的风险。

6. 使能 HTTPS

建议您开启 HTTPS，通过安全的通道访问 Web 服务。

7. 启用白名单

建议您开启白名单功能，开启后仅允许白名单列表中的 IP 访问设备。因此，请务必将您的电脑 IP 地址，以及配套的设备 IP 地址加入白名单列表中。

8. MAC 地址绑定

建议您在设备端将其网关设备的 IP 与 MAC 地址进行绑定，以降低 ARP 欺骗风险。

9. 合理分配帐户及权限

根据业务和管理需要，合理新增用户，并合理为其分配最小权限集合。

10. 关闭非必需服务，使用安全的模式

如果没有需要，建议您关闭 SNMP、SMTP、UPnP 等功能，以降低设备面临的风险。

如果有需要，强烈建议您使用安全的模式，包括但不限于：

- SNMP：选择 SNMP v3，并设置复杂的加密密码和鉴权密码。
- SMTP：选择 TLS 方式接入邮箱服务器。

- FTP：选择 SFTP，并设置复杂密码。
- AP 热点：选择 WPA2-PSK 加密模式，并设置复杂密码。

11. 音视频加密传输

如果您的音视频数据包含重要或敏感内容，建议启用加密传输功能，以降低音视频数据传输过程中被窃取的风险。

12. 使用 PoE 方式连接设备

如果设备支持 PoE 功能，建议采用 PoE 方式连接设备，使摄像机与其他网络隔离。

13. 安全审计

- 查看在线用户：建议您不定期查看在线用户，识别是否有非法用户登录。
- 查看设备日志：通过查看日志，可以获知尝试登录设备的 IP 信息，以及已登录用户的关键操作信息。

14. 网络日志

由于设备存储容量限制，日志存储能力有限，如果您需要长期保存日志，建议您启用网络日志功能，确保关键日志同步至网络日志服务器，便于问题回溯。

15. 安全网络环境的搭建

为了更好地保障设备的安全性，降低网络安全风险，建议您：

- 关闭路由器端口映射功能，避免外部网络直接访问路由器内网设备的服务。
- 根据实际网络需要，对网络进行划区隔离：若两个子网间没有通信需求，建议使用 VLAN、网闸等方式对其进行网络分割，达到网络隔离效果。
- 建立 802.1x 接入认证体系，以降低非法终端接入专网的风险。
- 启用设备的防火墙或者黑白名单功能，降低设备可能遭受攻击的风险。