



工业音频算法舱

操作手册

法律声明

版权所有©杭州海康威视数字技术股份有限公司 2022。保留一切权利。

本手册的任何部分，包括文字、图片、图形等均归属于杭州海康威视数字技术股份有限公司或其关联公司（以下简称“海康威视”）。未经书面许可，任何单位或个人不得以任何方式摘录、复制、翻译、修改本手册的全部或部分。除非另有约定，海康威视不对本手册提供任何明示或默示的声明或保证。

关于本产品

本手册描述的产品仅供中国大陆地区销售和使用。本产品只能在购买地所在国家或地区享受售后服务及维保方案。

关于本手册

本手册仅作为相关产品的指导说明，可能与实际产品存在差异，请以实物为准。因产品版本升级或其他需要，海康威视可能对本手册进行更新，如您需要最新版手册，请您登录海康威视官网查阅（<http://www.hikvision.com>）。

海康威视建议您在专业人员的指导下使用本手册。

商标声明

- **HIKVISION 海康威视** 为海康威视的注册商标。
- 本手册涉及的其他商标由其所有人各自拥有。

责任声明

- 在法律允许的最大范围内，本手册以及所描述的产品（包含其硬件、软件、固件等）均“按照现状”提供，可能存在瑕疵或错误。海康威视不提供任何形式的明示或默示保证，包括但不限于适销性、质量满意度、适合特定目的等保证；亦不对使用本手册或使用海康威视产品导致的任何特殊、附带、偶然或间接的损害进行赔偿，包括但不限于商业利润损失、系统故障、数据或文档丢失产生的损失。
- 您知悉互联网的开放性特点，您将产品接入互联网可能存在网络攻击、黑客攻击、病毒感染等风险，海康威视不对因此造成的产品工作异常、信息泄露等问题承担责任，但海康威视将及时为您提供产品相关技术支持。
- 使用本产品时，请您严格遵循适用的法律法规，避免侵犯第三方权利，包括但不限于公开权、知识产权、数据权利或其他隐私权。您亦不得将本产品用于大规模杀伤性武器、生化武器、核爆炸或任何不安全的核能利用或侵犯人权的用途。
- 如本手册内容与适用的法律相冲突，则以法律规定为准。

前言

本节内容的目的是确保用户通过本手册能够正确使用产品，以避免操作中的危险或财产损失。在使用此产品之前，请认真阅读产品手册并妥善保存以备日后参考。

本手册适用于工业音频算法舱（简称设备），介绍通过浏览器访问和配置设备的各项操作。

符号约定

对于文档中出现的符号，说明如下所示。

符号	说明
 说明	说明类文字，表示对正文的补充和解释。
 注意	注意类文字，表示提醒用户一些重要的操作或者防范潜在的伤害和财产损失危险。如果不加避免，有可能造成伤害事故、设备损坏或业务中断。
 危险	危险类文字，表示有高度潜在风险，如果不加避免，有可能造成人员伤亡的重大危险。

目 录

第 1 章 产品简介 1

 1.1 产品说明 1

 1.2 重点功能 1

第 2 章 激活设备 2

 2.1 通过浏览器激活 2

 2.2 通过 SADP 软件激活 4

 2.3 登录 6

 2.3.1 浏览器登录 6

 2.3.2 插件安装说明 7

 2.3.3 重置密码 7

 2.3.4 开启账户锁定 7

第 3 章 智能功能 9

 3.1 开启智能功能 9

 3.2 设置监控点参数 9

 3.3 工业音频诊断 9

 3.3.1 配置通道规则 9

 3.3.2 查看与下载故障音频 10

第 4 章 预览 11

 4.1 音频预览与录制 11

第 5 章 存储配置 12

 5.1 配置网络硬盘 12

 5.2 配置云存储 12

 5.3 配置 FTP 13

 5.4 存储卡配置 14

 5.4.1 配置本地存储盘 14

5.4.2 配置存储卡	15
5.4.3 校验存储卡	16
5.4.4 检测 MicroSD 卡状态	16
第 6 章 事件和报警	17
6.1 普通事件	17
6.1.1 配置报警输入	17
6.1.2 配置异常报警	17
第 7 章 计划和联动配置	19
7.1 布防时间配置	19
7.2 联动配置	19
7.2.1 联动 FTP/NAS/MicroSD 卡	19
7.2.2 联动上传中心	20
7.2.3 联动报警输出	20
第 8 章 网络配置	22
8.1 TCP/IP 参数	22
8.1.1 多播设置	23
8.2 设置端口参数	23
8.3 设置端口映射	23
8.3.1 设置自动端口映射	24
8.3.2 设置手动端口映射	24
8.3.3 设置路由器端口映射	24
8.4 设置萤石云访问	25
8.4.1 通过浏览器开启萤石云	25
8.4.2 通过 SADP 开启萤石云	26
8.4.3 通过萤石手机 APP 访问	26
8.5 设置 ISUP	27

8.6 网络服务	28
8.7 设置报警服务器	28
8.8 无线拨号	28
8.8.1 设置无线拨号	29
8.9 流量整形	29
8.10 流量监控	29
第 9 章 系统和安全参数	31
9.1 查看设备信息	31
9.2 恢复设备参数	31
9.3 查询和导出日志	31
9.4 导入/导出配置参数	32
9.5 导出诊断信息	32
9.6 重启设备	32
9.7 升级设备	32
9.8 设置自动维护	33
9.9 查看开源码授权信息	33
9.10 设置预览连接数	33
9.11 设置时间	33
9.11.1 手动校时	34
9.11.2 设置 NTP 校时	34
9.11.3 设置夏令时	34
9.12 设置 RS-485 参数	35
9.13 安全配置	35
9.13.1 设置认证方式	35
9.13.2 SSH	36
9.13.3 开启账户锁定	36
9.13.4 控件超时配置	36

9.13.5 证书管理 36

9.13.6 设置 HTTPS 39

9.13.7 安全审计日志 40

9.13.8 设置 QoS 41

9.14 管理设备用户 42

9.14.1 设置用户账户和权限 42

9.14.2 查看在线用户 43

9.14.3 设备同时登录数 43

第 1 章 产品简介

1.1 产品说明

工业音频算法舱（以下简称设备）应用于能源、制造业、石化、钢铁、电力等多种存在音频振动异常的工业场景。设备可搭配不同采集端子，实现不同场景的声纹分析和推理。

设备支持自行标定音频故障类型，可以分析故障类型并上报。

1.2 重点功能

介绍设备的重要功能，根据使用需求启用功能，请以实际设备为准。

工业音频诊断

设备支持边缘分析和推理功能，单通道能够分析故障类型并支持故障上报。

事件功能

设备支持普通事件。

第 2 章 激活设备

网络访问中，为了保护个人账户安全和隐私，提高设备的安全性，首次登录时，需设置 admin 用户密码激活设备。

激活方式如下。

表 2-1 激活方式

激活方式	说明	适用场景
通过浏览器激活	通过计算机端浏览器，激活设备。	适用于单台设备激活。
通过 SADP 软件激活	通过海康威视提供的 SADP 软件，搜索并激活与计算机处于同一局域网的设备。	适用于单台和多台设备激活。

2.1 通过浏览器激活

通过浏览器访问并激活设备。

操作步骤

1. 将设备连接到计算机所在的局域网中，设置计算机的 IP 地址与设备处于同一网段。计算机 IP 地址的设置请参考。



说明

设备出厂 IP 地址：192.168.1.64，计算机 IP 地址可以设置为 192.168.1.2~192.168.1.253 之间的任意一个 IP 地址（除 192.168.1.64 之外），例如：将计算机 IP 地址设置为 192.168.1.100。

2. 在浏览器中输入 192.168.1.64，显示激活界面。
3. 在激活设备处设置设备激活密码。



注意

- 为保护您的个人隐私和企业数据，避免设备的网络安全问题，建议您设置符合安全规范的高强度密码。
- 为了提高设备网络使用的安全性，设置的密码长度需达到 8~16 位，至少由数字、小写字母、大写字母和特殊字符中的 2 种或 2 种以上类型组合而成，且密码中不能包含用户名。

4. 单击确定。

设备的 admin 用户密码为激活时所设置的密码。

5. 可选操作: 根据界面提示, 选择安全问题或安全邮箱方式配置安全信息。



为了保障账号安全, 建议至少选择 1 种方式, 用于重置密码。登录设备后, 如需设置, 可通过 **配置 → 系统 → 用户管理**, 单击**账号安全设置**, 填写安全问题或安全邮箱的对应信息。

6. 可选操作: 开启萤石云。

- 1) 在浏览器中输入设备 IP 地址, 进入登录界面, 输入用户名和密码, 登录设备。
- 2) 进入 **配置 → 网络 → 高级配置 → 平台接入**。
- 3) 选择平台接入方式为**萤石云**。
- 4) 勾选**启用**。
- 5) 设置萤石云接入参数。

接入服务器 IP

默认

设备会根据就近区域的服务器自动分配一个服务器地址。

自定义

手动设置域名服务器地址。

验证码

为了设备访问的安全性, 请自定义设置一个验证码或修改原验证码, 用于将设备添加到萤石云帐号中。



验证码须为 6~12 位字母或数字, 区分大小写, 为保证设备安全, 建议设置 8 位以上的大小写字母和数字组合。

6) 单击**保存**。

注册状态显示在线, 表示设备已注册到萤石云平台。

7. 可选操作: 修改与重置密码。



- 为避免安全风险, 请定期以 admin 用户登录, 完成管理员密码修改, 具体可参考。
- 当 admin 用户忘记密码时, 单击修改网络参数界面的忘记密码, 可重置密码, 具体可参考。

后续处理

激活后, 在登录界面输入用户名和密码, 登录设备。如需修改设备网络信息, 进入 **配置 → 网络 → 基本配置 → TCP/IP**, 修改设备 IP 地址、子网掩码、网关等网络信息。

2.2 通过 SADP 软件激活

通过计算机上的 SADP 软件，搜索并激活与计算机处于同一局域网的设备。

前提条件

访问海康威视官网，进入 **服务支持** → **下载中心** → **桌面应用软件** → **Hikvision Tools**（含 SADP、录像容量计算等工具），获取 SADP 软件。也可直接访问以下网址下载：<https://www.hikvision.com/cn/support/Downloads/Desktop-Application/HikvisionTools/>，完成安装。

操作步骤

1. 将设备连接到安装有 SADP 软件的计算机所在的局域网中，或使用网线直接连接设备和计算机。
2. 运行 SADP 软件，单击**刷新**。
界面展示与计算机在同一局域网内的在线设备。
3. 选择列表中需要激活，且**激活状态**为**未激活**的设备。
4. 在**激活设备**处设置设备激活密码。



注意

- 为保护您的个人隐私和企业数据，避免设备的网络安全问题，建议您设置符合安全规范的高强度密码。
- 为了提高设备网络使用的安全性，设置的密码长度需达到 8~16 位，至少由数字、小写字母、大写字母和特殊字符中的 2 种或 2 种以上类型组合而成，且密码中不能包含用户名。

-
5. **可选操作**: 对于支持萤石云设备，可开启萤石云。

- 1) 勾选**使用萤石云**。
- 2) 设置验证码，用于将设备添加到萤石云帐号中。



说明

验证码须为 6~12 位字母或数字，区分大小写，为保证设备安全，建议设置 8 位以上的大小写字母和数字组合。

-
- 3) 单击**确定**。



图 2-1 开启萤石云

6. 单击**确定**。



图 2-2 激活设备

- 设备**激活状态**更新为**已激活**。
- 设备的 admin 用户密码为激活时所设置的密码。

7. 可选操作: 根据界面提示, 选择安全问题或安全邮箱方式配置安全信息。

 说明

为了保障账号安全, 建议至少选择 1 种方式, 用于重置密码。登录设备后, 如需设置可设备, 通过 **配置** → **系统** → **用户管理**, 单击**账号安全设置**, 填写**安全问题**或**安全邮箱**的对应信息。

8. 可选操作: 修改与重置密码。



- 为避免安全风险，请定期以 admin 用户登录，完成管理员密码修改，具体可参考。
- 当 admin 用户忘记密码时，单击修改网络参数界面的忘记密码，可重置密码，具体可参考。

后续处理

如需修改设备网络信息，可选择已激活的设备，进入 **修改网络参数**，设置设备的 IP 地址、子网掩码、网关等信息，输入 admin 用户密码，单击 **修改**，保存参数。



图 2-3 修改设备信息

2.3 登录

2.3.1 浏览器登录

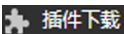
通过浏览器登录设备，插件安装的方法。

操作步骤

1. 在浏览器中输入设备的 IP 地址，弹出登录画面。
2. 设备提示安装浏览器插件。根据界面提示，安装插件。
3. 再次打开浏览器，输入设备的 IP 地址。
4. 输入用户名和密码，单击 **登录**。
5. 可选操作: 单击 **注销**，安全退出登录。

2.3.2 插件安装说明

通过不同的操作系统、浏览器登录设备时，可能会有不同的功能显示，为了保证功能正常显示和使用时，请根据使用情况安装插件或设置参数，请以实际设备界面为准。

操作系统	浏览器版本	安装插件操作
Windows	• IE 10 ~11 • Google Chrome 56 及以下版本 • Mozilla Firefox 51 及以下版本	请根据系统提示完成插件的安装。
	• Google Chrome 57 及以上版本 • Mozilla Firefox 52 及以上版本	单击预览页面，单击  插件下载，下载并安装插件，可以获得高质量的显示并完成设备功能操作。

2.3.3 重置密码

通过配置账号安全信息，当 admin 用户忘记密码时，单击登录界面的忘记密码，可重置密码。您可通过安全问题或安全邮箱，重置 admin 用户的密码。



说明

重置 admin 用户密码时，请确保设备和计算机的 IP 在同一局域网网段。

安全问题

在激活时进行账号安全设置，或通过 **配置 → 系统 → 用户管理**，单击**账号安全设置**，选择安全问题，并填写问题的答案。

安全邮箱

在激活时进行账号安全设置，或通过 **配置 → 系统 → 用户管理**，单击**账号安全设置**，选择安全邮箱，并填写安全邮箱信息。

2.3.4 开启账户锁定

用于提升设备网络访问的安全性。

admin 用户可以设置密码错误尝试次数和锁定时间。当密码输入错误达到限定的次数，设备将自动锁定。达到设置的锁定时间后，设备自动解锁。

通过 **配置 → 系统 → 安全管理 → 安全服务**，勾选**开启非法登录锁定**，设置**错误尝试次数**和**锁定时间**。

第 3 章 智能功能

介绍设备支持的智能功能及配置。

3.1 开启智能功能

不同智能功能对应不同的智能资源。当需要使用某种智能功能时，请开启对应的智能资源。

操作步骤

1. 进入 **应用仓库** → **智能资源分配**。
2. 选择需要开启的智能资源。
3. 单击 **保存**。



说明

- 部分智能功能互斥，当某个智能功能的资源开启后，与其互斥的智能功能将被隐藏。
 - 切换智能资源后，需重启设备生效。
-

3.2 设置监控点参数

设置场景中各个监控点的参数，方便对各个监测点进行管理。

通过 **应用仓库** → **通用智能配置** → **监控点信息**，设置监控点参数，单击 **保存**。

3.3 工业音频诊断

通过 AI 平台，可将已完成训练的算法模型部署到设备中，再结合设备中已有的算法，实现检测分类任务。

3.3.1 配置通道规则

操作步骤

1. 进入 **应用仓库** → **工业音频诊断** → **工业听诊**。
2. 选择通道号。
3. 设置音频。导入或添加已知的音频样本，设备模型诊断出的故障音频将与样本进行二次比对，最终判断是否为故障音频。
 - 导入外部音频样本

- a. 在 **音频设置** 中单击 **导入**，可选择外部音频样本文件导入。
- b. 单击 **浏览**，选择本地的音频样本。
- c. 设置该样本类别为 **正常样本** 或 **故障样本**。
- d. 自定义编辑音频样本的名称。
- e. 单击 **确定** 完成导入。
- 添加设备已录制的音频样本
 - a. 在 **音频设置** 中单击 **添加**，可选择现有故障音频文件。
 - b. 单击 **确定** 完成导入。
4. 设置布防时间请参见 **布防时间配置**，设置规则联动请参见 **联动配置**。
5. 单击 **保存** 完成配置。

后续处理

重复上述步骤可配置其他通道参数。

3.3.2 查看与下载故障音频

用于查询、回放和下载已存储的故障音频。

操作步骤

1. 单击 **故障音频**。
2. 设置搜索条件，单击 **查找**。

符合条件的文件将显示在故障音频文件列表中。
3. 选中需要查看的文件，单击 **下载**。



说明

可进入 **配置** → **本地**，在 **下载保存路径** 中，单击 **浏览** 更改保存路径。

第 4 章 预览

介绍设备预览时，预览参数、功能图标参数、传输参数等调节。

4.1 音频预览与录制

介绍设备预览界面的操作。

操作步骤

1. 在设备主界面上，点击通道号，可进行声音实时播放，并展示声音波形图。
2. 点击  开始录音，再次点击停止录音。

后续处理

音频文件存储路径可进入 **配置** → **本地**，在 **音频文件保存路径**中配置。

第 5 章 存储配置

介绍介绍设备几种常用的存储路径的设置方法。

5.1 配置网络硬盘

将网络中的服务器作为网络硬盘，存储音频文件。

前提条件

请先获取网络硬盘服务器地址。

操作步骤

1. 进入 **配置** → **存储** → **存储管理** → **网络硬盘**。
2. 设置服务器地址和文件路径。

服务器地址

网络硬盘的 IP 地址。

文件路径

网络硬盘内的文件保存路径。

3. 设置挂载方式，可选 **NFS** 和 **SMB/CIFS**。当挂载方式选择为 **SMB/CIFS** 时，需设置认证的用户名和密码。
4. 单击**测试**，查看设置的网络硬盘是否可用。
5. 单击**保存**。

5.2 配置云存储

用于将音频文件和信息上传至云端，平台可直接向云端请求文件，可更快速的进行文件查看及分析，该功能请以实际设备为准。

操作步骤



注意

云存储开启时，文件优先存储在云存储服务器上。

1. 进入 **配置** → **存储** → **存储管理** → **云存储**。
2. 勾选**启用云存储**。
3. 设置基本参数。

协议版本

云存储服务器的协议版本。

接入服务器 IP	云存储服务器的地址，支持 IPv4 地址。
接入服务器 Port	云存储服务器的端口，缺省为 6011，不建议修改。
用户名和密码	云存储服务器的用户名和密码。
密码确认	重复输入密码进行密码确认。
接入密钥	登录云存储服务器的密钥。
加密密钥	对于存储到云存储服务器上的数据进行加密的密钥。
数据池 ID	云存储服务器端存储设备上传文件的存储区域编号。需要确保数据池 ID 和云存储服务器的存储区域编号一致。



说明

用户名、密码、密码确认，接入密钥和加密密钥视云存储协议而定，请以实际的协议版本为准。

- 4. 单击 **测试**，测试所配置的云存储是否正确。
- 5. 单击 **保存**。

5.3 配置 FTP

通过音频分析获取到音频文件，将文件上传到指定的 FTP 服务器上存储。

前提条件

请先获取 FTP 服务器地址。

操作步骤

- 1. 单击 **配置** → **网络** → **高级配置** → **FTP 设置**。
- 2. 设置 FTP 参数。

FTP 协议

可选择 FTP 和 SFTP。使用 SFTP 将通过加密的方式传输文件，相对更安全。

服务器地址和端口

表示 FTP 服务器地址和对应的端口。

用户名和密码

表示具备上传权限的用户名和密码。

如果匿名用户也具备上传权限，可勾选 **匿名登录**，则设备通过匿名方式访问 FTP 服务器。

目录结构

表示文件在 FTP 服务器上的保存路径。

数据归档间隔

在 FTP 服务器上自动生成文件夹，将音频文件以天为单位进行存档，方便后续检索。

如果归档间隔设置为 1 天，设备将以“年_月_日-年_月_日”为名称，每天生成 1 个文件夹。依此类推，如果归档间隔设置为 2 天，则设备每 2 天生成 1 个文件夹。

数据名

根据需求设置 FTP 的文件名。选择默认时，文件将以设备的 IP 地址为前缀。



配置参数项视型号而定，请以实际设备为准。

- 3. 可选操作: 勾选 **上传音频文件**，开启上传音频文件至 FTP 的功能。
- 4. 可选操作: 勾选 **启用断网续传**。

断网续传

当设备的网络出现异常的时候，将数据自动缓存至设备 SD 卡，待网络恢复正常，设备将上传断网缓存的数据。

- 5. 可选操作: 单击 **测试**，查看设置的 FTP 服务器是否可用。
- 6. 单击 **保存**。

5.4 存储卡配置

设备配置存储卡后可对音频、数据等内容进行本地存储。存储过程中，可实时查看存储卡的容量、剩余空间和状态等。同时支持对所有类型的 microSD 卡进行加密存储，有效提升存储安全性。

5.4.1 配置本地存储盘

设备内置本地存储盘，当未另外安装 microSD 卡或 microSD 卡状态异常时，可将音频文件存储到本地存储盘中。

操作步骤



当设备安装有 microSD 卡，且 microSD 卡状态正常时，本地存储盘将不生效。

- 1. 进入 **配置 → 存储 → 存储管理 → 硬盘管理**。
- 2. 根据需求选择是否对本地存储盘进行格式化或加密。

格式化 勾选检测到的本地存储盘（磁盘号为 2），单击 **格式化**。

加密格式化 格式化后通过设置加密密码进行加密存储。
勾选检测到的本地存储盘（磁盘号为 2），单击**加密格式化**并设置加密密码。
加密格式化成功后，**状态**显示为**已加密**。此时，本地存储盘可进行加密存储。



说明

- 加密密码不支持修改，只能重新加密格式化，建议妥善保管。
- 已加密的本地存储盘，单击**格式化**可切换为不加密状态。格式化操作会导致存储数据丢失，请先备份数据。

3. 可选操作: 配置磁盘配额，请根据需要设置不同类别数据和文件的存储百分比。
4. 单击**保存**。

5.4.2 配置存储卡

存储到 microSD 卡时，需要先进行 microSD 卡的安装及格式化。当 microSD 卡状态正常后，可将音频文件存储到 microSD 卡上。

前提条件

设备插入 1 张未加密的 microSD 卡或全新的 microSD 卡。microSD 卡安装操作请参见设备的**快速入门指南**。

操作步骤

1. 进入 **配置** → **存储** → **存储管理** → **硬盘管理**。
2. 格式化 microSD 卡，并根据需求选择是否对卡进行加密。

格式化 勾选检测到的 microSD 卡，单击**格式化**。
格式化成功后，**状态**显示为**正常**。此时，microSD 卡可进行正常存储。

加密格式化 存储卡格式化后通过设置加密密码进行加密存储。支持对所有类型的 microSD 卡进行加密存储。
勾选检测到的 microSD 卡，单击**加密格式化**并设置加密密码。
加密格式化成功后，**状态**显示为**已加密**。此时，microSD 卡可进行加密存储。



说明

- 加密密码不支持修改，只能重新加密格式化，建议妥善保管。
- 已加密的 microSD 卡，单击**格式化**可切换为不加密状态。格式化操作会导致存储卡数据丢失，请先备份数据。

3. 可选操作: 配置磁盘配额，请根据需要设置不同类别数据和文件的存储百分比。

4. 单击 **保存**。

5.4.3 校验存储卡

当设备插入 1 张已加密的 microSD 卡，需通过校验输入 microSD 卡正确的加密密码。校验成功后，microSD 卡才能正常使用。

前提条件

设备插入 1 张已加密的 microSD 卡。

操作步骤

1. 进入 **配置** → **存储** → **存储管理** → **硬盘管理**。
2. 勾选待校验的 microSD 卡，单击 **校验**。
3. 输入正确的加密密码，单击 **确定**。

校验成功后，**状态**显示为**已加密**。

4. **可选操作**: 配置磁盘配额，请按需设置不同类别数据和文件的存储百分比。
5. 单击 **保存**。

5.4.4 检测 MicroSD 卡状态

对海康威视 MicroSD 卡状态进行检测。当 MicroSD 卡出现异常时，能够及时得到状态变化的反馈。

前提条件

请在设备中安装 MicroSD 卡。

操作步骤

1. **配置** → **存储** → **存储管理** → **SD 卡状态检测**。
2. 设置布防时间和联动方式，详细请参见 [布防时间配置](#) 和 [联动配置](#)。
3. 单击 **保存**。

单击 **健康监测**，查看 MicroSD 卡预计剩余寿命和健康状态。

4. **可选操作**: 单击 **读写锁定**，可设置 MicroSD 卡的读写权限。
 - 1) 将锁定开关选择为**开启**。
 - 2) 设置锁定密码。
 - 3) 单击 **保存**。



说明

- 读写锁定仅限 admin 用户登录设置。
 - 锁定状态的 MicroSD 卡不可读写。
-

第 6 章 事件和报警

介绍设备支持的各个事件的功能配置，根据需求配置相应的事件，触发设备执行联动动作。

6.1 普通事件

介绍设备基本的事件配置。

6.1.1 配置报警输入

设备的报警输入接口外接报警设备，当外接报警设备产生报警信号时，触发设备执行联动动作。

前提条件

设备的报警输入接口外接报警设备，接线方法请参见 *快速入门指南*。

操作步骤



说明

报警输入功能视型号而定，请以实际设备为准。

1. 进入 **配置** → **事件** → **普通事件** → **报警输入**。
2. 勾选 **处理报警输入**。
3. 选择 **报警输入号**和**报警类型**，填写**报警名称**。



说明

根据连接的报警设备设置报警类型。

4. 布防时间设置请参见 **布防时间配置**，联动方式设置请参见 **联动配置**。
5. 单击 **复制到**，复制该报警输入设置信息至其他的报警输入通道。
6. 单击 **保存**。

6.1.2 配置异常报警

当设备出现网络断开等异常情况时，触发设备执行联动动作。

操作步骤

1. 进入 **配置** → **事件** → **普通事件** → **异常**。
2. 根据需求，选择**异常类型**。

硬盘错误 表示设备中安装的存储设备状态出现错误时触发联动动作。

网线断开 表示设备没有连接网线或网线脱落时触发联动动作。

IP 地址冲突 表示设备 IP 地址与网络中的其它设备 IP 地址相同时触发联动动作。

非法访问 表示设备输入错误的用户名或密码时触发联动动作。

3. 联动方式设置请参见 **联动配置**。

4. 单击 **保存**。

第 7 章 计划和联动配置

设备在设置的时间段内执行对应的操作，如：录音、布防。通过联动使设备执行相应的动作。

7.1 布防时间配置

设置任务执行的开始时间和结束时间。

操作步骤

1. 选中时间轴上的某点为起始点，按住鼠标左键在时间轴上拖动，拖动到结束点时松开鼠标，完成布防时间设置。



说明

一条时间轴上支持设置 8 个时间段。

2. 调整布防时间。
 - 单击布防时间段，可手动输入开始时间和结束时间调整布防时间，单击 **保存**。
 - 单击布防时间段，时间段两端会显示两个圆圈，鼠标移动到时间段的两端，会显示左右方向的调节箭头，移动调节箭头可调整时间段。
 - 鼠标拖动布防时间段到时间轴上的任一位置，可以重设时间段。

单击时间段的 **删除** 删除当前时间段。

单击 **删除** 删除选中的时间段。

单击 **删除全部** 删除设置的所有时间段。

3. 可选操作: 单击时间轴右侧出现的 ，复制相同的布防时间到其它时间。
4. 单击 **保存**。

7.2 联动配置

当有事件或报警发生时可开启报警联动。



说明

设备支持的联动方式视型号而定，请以实际设备为准。

7.2.1 联动 FTP/NAS/MicroSD 卡

若勾选并配置好 FTP/NAS/MicroSD 卡，当触发报警时，可将报警信息发送到 FTP 服务器、网络硬盘或 MicroSD 卡中进行保存。

配置 FTP 服务器存储，请参见 [配置 FTP](#)。

配置 NAS 存储，请参见 [配置网络硬盘](#)。

配置 MicroSD 卡存储，请参见 [配置存储卡](#)。

7.2.2 联动上传中心

勾选**上传中心**，当发生报警时，可将报警信息、图片等信息上传到远程的监控中心。

7.2.3 联动报警输出

设备的报警输出接口中连接了报警输出设备，勾选且配置好对应的报警输出通道，当触发报警时，报警信息将从连接的报警输出设备中输出。

操作步骤

说明

报警输出视型号而定，请以实际设备为准。

1. 进入 **配置** → **事件** → **普通事件** → **报警输出**。

2. 设置报警参数。

自动报警输出 设置方法请参见 [自动报警](#)。

手动报警输出 设置方法请参见 [手动报警](#)。

3. 单击**保存**。

自动报警

若需在设置的布防时间内触发报警输出，请配置自动报警。

操作步骤

1. 设置自动报警参数。

报警输出号

根据外接报警设备连接的报警接口选择报警输出号。

延时

表示产生报警后，延长多长时间关闭报警，请根据实际需求进行选择。

说明

当选择为**手动**，当产生报警后，请单击**手动报警**和**清除报警**，关闭报警。

报警名称

自定义报警名称。

2. 设置布防时间，具体设置请参考 [布防时间配置](#)。
3. 单击时间轴右侧出现的 ，设置其他报警输出通道的报警参数一致。
4. 单击 **确定**。

手动报警

通过手动触发报警输出。

操作步骤

1. 设置手动报警参数。

报警输出号

根据外接报警设备连接的报警接口选择报警输出号。

报警名称

自定义报警名称。

2. 单击 **手动报警**，开启手动触发报警输出。



说明

单击 **清除报警**，关闭手动报警的报警输出。

第 8 章 网络配置

介绍网络参数的配置方法。

8.1 TCP/IP 参数

配置设备的 TCP/IP 参数，使设备能在网络中正常使用。

选择 **配置** → **网络** → **基本配置** → **TCP/IP**，设置设备的基本网络参数，并单击 **保存**。

网卡类型

根据网络环境选择。

IPv4 地址

勾选 **自动获取**，设备将根据网络环境自动获取网络参数。



注意

当设备网络支持 DHCP（Dynamic Host Configuration Protocol）服务器，且设备为自动获取 IP 地址方式时，设备 IP 地址会被修改。可通过 SADP 工具来获取设备的 IP 地址。

不勾选 **自动获取**，需手动填写设备 **IPv4 地址**、**IPv4 子网掩码**和 **IPv4 默认网关**等局域网参数信息。



说明

手动填写 IPv4 网络参数时，单击 **测试**可确认该 IP 地址是否可用。

IPv6 地址

请根据需求填写 IPv6 网络参数，如不明确请咨询网络管理人员。

- 路由公告模式使用公告的 IP 前缀加设备自身的物理地址生成 IPv6 地址。
- 自动获取模式由相应的服务器、路由或网关下发 IPv6 地址。
- 手动模式根据实际网络需要配置，如不明确请咨询网络管理人员。

MTU

表示最大传输单元，是指 TCP/UDP 协议网络传输中所通过的最大数据包的大小。

DNS

当设备设置了正确可用的 DNS 服务器地址后，可通过域名对设备进行访问。

动态域名

勾选 **启用动态域名** 并配置注册域名后，局域网中可以通过该注册域名搜索并访问设备。



请先通过 **配置 → 网络 → 基本配置 → TCP/IP** 勾选 **自动获取**。动态域名在开启自动获取 (DHCP) 后生效。

8.1.1 多播设置

勾选 **启用多播搜索**，设备将支持以多播方式被网络内其他设备发现。



当因多播风暴引起设备无法正常使用时，您可尝试关闭多播搜索缓解问题。

8.2 设置端口参数

当设备因端口冲突导致无法进行网络访问时，可修改设备端口。



请不要随意修改缺省端口参数，否则会导致设备无法访问。

进入 **配置 → 网络 → 网络服务**，设置端口参数，保存后生效。

HTTP 端口

表示浏览器访问设备的端口。如当 **HTTP 端口** 修改为 **81** 时，使用浏览器登录时，需要在浏览器输入 `http://192.168.1.64:81` 进行访问。

RTSP 端口

表示设备实时传输协议的端口。

HTTPS 端口

表示浏览器证书访问的端口，当浏览器访问设备时，需要通过证书验证才能访问，安全级别高。

8.3 设置端口映射

通过设置端口映射，可以访问指定端口的设备。

前提条件

当前设备中的端口与网络中的其它设备端口相同时，请参见 **修改设备端口**。

操作步骤

1. 进入 **配置** → **网络** → **基本配置** → **端口映射**。
2. 选择端口映射方式，设置设备端口映射。

自动映射 设置方法请参见 [设置自动端口映射](#)。

手动映射 设置方法请参见 [设置手动端口映射](#)。

3. 单击 **保存**。

8.3.1 设置自动端口映射

自动分配设备和路由器上的端口映射，实现设备端口开放。

操作步骤

1. 勾选 **启用 UPnP™**，可根据需求设置一个别名。
2. 端口映射方式选择 **自动**。
3. 单击 **保存**。



说明

路由器上同时开启 UPnP™ 功能。

8.3.2 设置手动端口映射

手动设置设备和路由器上的端口映射，实现设备端口开放。

操作步骤

1. 勾选 **启用 UPnP™**，可根据需求设置一个别名。
2. 端口映射方式选择 **手动**，设置外部端口与内部端口相同。
3. 单击 **保存**。

后续处理

进入路由器端口映射界面，将端口号和 IP 地址设置成与设备中的一致。

8.3.3 设置路由器端口映射

通过路由器，将摄像机的局域网端口映射到互联网上。

前提条件

路由器安装调试完毕，并能保证正常接入互联网。

以一款 TP-LINK 路由器配置界面为例介绍端口映射方法，其他路由器的配置界面可能不同，请以实际路由器界面为准。

操作步骤

1. 在路由器的 **设置向导** 中选择上网方式。
2. 设置路由器 **网络参数** 中的 **LAN 口设置**，填写 **IP 地址** 和 **子网掩码**。



说明

IP 地址即为局域网的网关。

3. 在路由器的 **转发规则** → **虚拟服务器** 中，设置端口映射。



说明

摄像机的端口号不可与其他端口号冲突，若路由器的 web 管理端口号为 80，则需要修改路由器或网络摄像机的端口号来避免冲突。当修改摄像机的 HTTP 端口为 81，使用浏览器登录时，需要输入 `http://192.168.1.64:81` 进行访问。

将路由器的端口号映射给摄像机，访问路由器端口号即访问摄像机的端口号。

8.4 设置萤石云访问

萤石云为萤石旗下微视频服务平台。支持萤石云接入的设备，可将设备注册并添加到萤石云平台，并通过萤石云账号访问设备。萤石云支持情况视型号而定，请以实际设备为准。

前提条件

通过萤石云官网注册萤石云账号和密码。

操作步骤

1. 开启萤石云。

通过浏览器开启 详细操作参见 [通过浏览器开启萤石云](#)。

通过 SADP 开启 详细操作参见 [通过 SADP 开启萤石云](#)。

2. 通过萤石云视频 APP 访问，详细操作参见 [通过萤石手机 APP 访问](#)。

8.4.1 通过浏览器开启萤石云

设备通过浏览器可开启并设置萤石云功能，实现萤石云访问设备。

操作步骤

1. 进入 **配置** → **网络配置** → **高级配置** → **平台接入**。
2. 勾选 **启用**。
3. 平台接入方式选择为萤石云
4. 设置萤石云接入参数。

接入服务器 IP

默认表示设备会根据就近区域的服务器自动分配一个服务器地址。

自定义表示可手动设置域名服务器地址。

验证码

为了设备访问的安全性，请自定义设置一个验证码或修改原验证码，用于将设备添加到萤石云帐号中。



说明

验证码须为 6-12 位字母或数字，区分大小写，为保证设备安全，建议设置 8 位以上的大小写字母和数字组合。

5. 单击**保存**。

注册状态显示**在线**，表示设备已注册到萤石云平台。

8.4.2 通过 SADP 开启萤石云

介绍通过 SADP 软件可开启萤石云功能。

前提条件

通过 www.hikvision.com 获取 SADP 软件，并完成安装。

操作步骤

1. 打开 SADP 软件。
2. 勾选需要开启萤石云的设备，开启萤石云。
 - 选择未激活的设备，在激活时勾选**使用萤石云**，设置验证码，开启萤石云。
 - 选择已激活的设备，勾选**使用萤石云**，设置验证码，输入设备的密码，单击**修改**，开启萤石云。



说明

设备激活方法请参见 [通过 SADP 软件激活](#)。

8.4.3 通过萤石手机 APP 访问

通过萤石云视频 APP 可以将设备接入萤石云，通过手机 APP 访问设备。

前提条件

设备通过有线网络连接路由器，请保证路由器正常连接广域网。

操作步骤

1. 手机扫描萤石云视频 APP，下载、安装和注册客户端软件。



注意

下载操作会消耗流量，建议在 Wi-Fi 环境中进行。



图 8-1 萤石云视频二维码



说明

萤石云视频二维码支持 Android 系统或 iOS 系统的手机扫描下载。

- 单击客户端软件左上角的 $+$ ，添加设备。
 - 扫描设备机身或说明书上的二维码。
 - 单击软件右上角的 $\square$ ，手动输入设备标签上的序列号。
 - 选择**非萤石设备**，根据界面提示将设备接入萤石云。
-



说明

添加和配置操作要求在摄像机上电后的 3 分钟内完成，否则需要重启设备，重新操作。

- 单击**实时预览**，选择通道，访问设备。
-

8.5 设置 ISUP

遵循 ISUP（原 Ehome）平台的要求，将设备注册 ISUP 平台，实现远程实时监控、管理设备等功能。

操作步骤

- 进入 **配置** $\rightarrow$ **网络** $\rightarrow$ **高级配置** $\rightarrow$ **平台接入**。
- 平台接入方式选择为 ISUP。
- 勾选**启用**。
- 根据 ISUP 协议，设置 ISUP 参数。
- 单击**保存**。

刷新网页或者重启设备查看注册状态。

8.6 网络服务

请根据需求开启和关闭各类网络服务协议，该功能请以实际设备为准。

操作步骤

1. 进入 **配置 → 网络 → 高级配置 → 网络服务**。
2. 设置网络服务参数。

启用 **TLS1.1** 版本、启用 **TLS1.2** 版本或启用 **TLS1.3** 版本

勾选表示设备支持 TLS1.1 协议、TLS1.2 协议或 TLS1.3 协议访问设备。

3. 单击 **保存**。

8.7 设置报警服务器

设备通过 HTTP、HTTPS 或 ISUP 协议的方式发送报警信息给目的 IP 或域名。

操作步骤

1. 进入 **配置 → 网络 → 高级配置 → 报警服务器**。
2. 输入目的 **IP 或域名**、**URL 地址**和**端口**。



目的 IP 地址或域名需支持 HTTP、HTTPS 或 ISUP 协议传输。

3. 选择**协议类型**及是否启用**断网续传**。

断网续传

当设备的网络出现异常的时候，将数据自动缓存至设备 SD 卡，待网络恢复正常，设备将上传断网缓存的数据。

4. 单击 **测试**。



单击 **重置**，可重新设置目的 IP 地址或域名的信息。

5. 单击 **保存**。
-

8.8 无线拨号

互联网中需要快速高质量的传输音频、视频和图像等数据，可采用 3G、4G、5G 等拨号方式，将设备连接至互联网，该功能请以实际设备为准。

8.8.1 设置无线拨号

内置无线模块的设备，通过无线模块拨号，实现互联网访问。

前提条件

获取运营商的 SIM 卡，开通 3G/4G/5G 等服务，将 3G/4G/5G 卡等插入设备的对应卡槽内。

操作步骤

1. 进入 **配置** → **网络** → **基本配置** → **无线拨号**。
2. 勾选 **启用**。
3. 单击 **拨号参数**，配置并保存无线拨号参数。
4. 单击 **拨号计划**，配置方法请参见 **布防时间配置**。
5. 单击 **拨号状态**。

单击 **刷新** 刷新拨号状态。

单击 **断开** 断开 3G/4G/5G 拨号。

如果 **拨号状态** 显示 **connected**，表示拨号成功。

6. 选择互联网中的一台计算机，通过 **IP 地址** 访问设备。
 - 打开浏览器输入 IP 地址访问设备。
 - 在客户端软件添加时，选择 **普通 IP**，输入 IP 地址等参数，访问设备。

8.9 流量整形

启用流量整形，可使传输码流趋于平滑，数据以相对均匀的速率传输，以解决瞬时带宽过大导致网络拥塞造成的数据丢失和延迟等问题，保证音频预览时的流畅性。

整形系数可选择**高**、**中**、**低**三个等级，建议您根据实际网络情况选择。

说明

- 流量整形功能仅在协议类型为 **TCP** 或 **UDP** 时生效。前往 **配置** → **本地** → **播放参数** 可设置协议类型。
 - 该功能请以实际设备为准。
-

8.10 流量监控

用于查看、分析和管理设备的 SIM 卡流量或有线网络流量。**SIM** 卡流量常指网络运营商提供的流量服务，有线网络流量则常指通过 **4G** 路由器来连接的计算机网络服务。

操作步骤

1. 进入 **配置** → **网络** → **高级配置** → **流量监控**。
2. 勾选 **启用**。
3. 选择套餐，并设置套餐参数。

套餐类型

日套餐、月套餐、年套餐可选。

套餐流量

表示套餐包含的可用流量。需输入流量数值，选择流量单位。

预警阈值

表示流量使用达到多少（百分比）进入流量预警状态。流量达到预警阈值后，系统支持报警上传、预览 OSD 提醒、登录弹框提醒等方式进行流量预警。

4. 设置常规联动方式。

上传中心 勾选**上传中心**，可将预警信息上传至中心平台。

5. 单击 **保存**。



说明

功能视型号而定，请以实际设备为准。

后续处理

通过**流量使用统计**，查看流量具体使用情况。

第 9 章 系统和安全参数

介绍设备的系统维护、系统配置及安全管理等参数及相关参数设置。

9.1 查看设备信息

用于查看设备编号、设备型号、序列号和版本等设备信息。

通过 **配置 → 系统 → 系统设置 → 基本信息**，查看设备信息。



设备名称和编号可根据需求自定义。

9.2 恢复设备参数

介绍设备执行恢复默认参数的操作。

操作步骤

1. 进入 **配置 → 系统 → 系统维护 → 升级维护**。
2. 根据实际需求单击 **简单恢复**或**完全恢复**。

简单恢复 除用户信息、网络参数和视频制式等外，其他参数恢复至出厂状态，请谨慎使用。

完全恢复 恢复设备的所有全部参数至出厂状态，请谨慎使用。

9.3 查询和导出日志

当系统发生未知故障时，可通过参考日志及时定位和排查问题。

操作步骤

1. 进入 **配置 → 系统 → 系统维护 → 日志**。
2. 选择日志类型、开始时间和结束时间。
3. 单击 **查找**。

日志列表中显示符合查询条件的所有日志信息。

4. 单击 **导出**，可将日志保存到计算机上。

9.4 导入/导出配置参数

通过导入/导出设备的配置文件，获取设备的配置参数，方便用户对其它设备进行相同参数的配置。

导入配置参数

通过 **配置 → 系统 → 系统维护 → 升级维护**，选择参数导入中的设备参数，根据界面提示操作完成导入设备的配置参数。

导出配置参数

通过 **配置 → 系统 → 系统维护 → 升级维护**，选择信息导出中的设备参数，根据界面提示操作完成导出设备的配置参数。

9.5 导出诊断信息

介绍导出设备运行状态的诊断信息。诊断信息包括 3 个模块，分别为软件状态信息、硬件运行信息和启动日志信息。

通过 **配置 → 系统 → 系统维护 → 升级维护**，根据实际情况勾选诊断信息模块并单击**导出诊断信息**，导出设备诊断信息。

9.6 重启设备

介绍设备重启的操作。

通过 **配置 → 系统 → 系统维护 → 升级维护**，单击**重启**。

9.7 升级设备

介绍设备执行升级的操作。

前提条件

获取正确的升级包，并存放在计算机中。



注意

设备升级过程中请勿关闭电源，升级完成后设备会自动重启。

操作步骤

1. 进入 **配置 → 系统 → 系统维护 → 升级维护**。
2. 选择升级方法。

- 当明确知道升级文件存放的路径时，选择升级文件，单击**浏览**选择升级文件。
- 当文件夹中包含多种升级包时，选择升级目录，单击**浏览**选择升级文件存放的目录，设备将自动分辨目录下正确的升级文件。

3. 单击**升级**。

9.8 设置自动维护

若设备运行时间较长，您可以设置在每周空闲的时间进行设备重启。

前提条件

登录用户须为 admin 用户，其余用户无操作权限。

操作步骤



设备重启期间无法录像。

1. 进入 **配置 → 系统 → 系统维护 → 升级维护**。
2. 勾选**启用自动维护**，并根据界面提示单击**确定**。
3. 选择周内某一天，设置具体维护时间。
4. 单击**保存**。

设备在设定的维护周期内按计划重启。

9.9 查看开源码授权信息

用于查看设备开源码授权信息。

进入 **配置 → 系统 → 系统设置 → 关于设备**，单击**查看**。

9.10 设置预览连接数

在实况画面中，设备通道最多能预览的数量。

通过 **配置 → 系统维护 → 系统服务**，设置**预览连接数**，单击**保存**。

9.11 设置时间

通过设置时区、校时和夏令时的方式设置设备时间。

9.11.1 手动校时

用于手动设置设备时间。

操作步骤

1. 进入 **配置** → **系统** → **系统设置** → **时间配置**
2. 选择时区。
3. 单击 **手动校时**。
4. 选择校时方式。
 - 选择**设置时间**，手动输入或选择日历设置设备时间。
 - 勾选**与计算机时间同步**，保持设备与本地计算机的时间一致。
5. 单击 **保存**。

9.11.2 设置 NTP 校时

若需要使用准确且可靠的时间源进行校时，可使用 NTP 校时。

前提条件

请先搭建或获取 NTP 服务器信息。

操作步骤

1. 进入 **配置** → **系统** → **系统设置** → **时间配置**。
2. 选择时区。
3. 单击 **NTP 校时**。
4. 填写**服务器地址**、**NTP 端口**和**校时时间间隔**。



服务器地址为 NTP 服务器的 IP 地址或域名。

5. 单击**测试**，判断设备与 NTP 服务器之间正常连接。
6. 单击 **保存**。

9.11.3 设置夏令时

若设备所处地区实行夏令时制，可通过配置夏令时，将设备与当地时间保持同步。该功能请以实际设备为准。

操作步骤

1. 进入 **配置** → **系统** → **系统设置** → **夏令时**。
2. 勾选**启用夏令时**。
3. 根据设备所处地区夏令时制选择**开始时间**、**结束时间**和**偏移时间**。

4. 单击 **保存**。



说明

夏令时功能视型号而定，请以实际设备为准。

9.12 设置 RS-485 参数

RS-485 可用于接入控制信号。

前提条件

使用 RS-485 线缆，连接设备和计算机或终端。

操作步骤

1. 进入 **配置 → 系统 → 系统设置 → RS-485**。
2. 根据使用需求设置 RS-485 参数，请保持设备和计算机或终端的参数一致。
3. 单击 **保存**。



说明

RS-485 功能视型号而定，请以实际设备为准。

9.13 安全配置

介绍设备安全相关的参数设置，可以提高系统的安全性。

9.13.1 设置认证方式

设置 RTSP 认证和 WEB 认证，可提高网络访问的安全性。

通过 **配置 → 系统 → 安全管理 → 认证方式**，选择所需认证协议和认证方式。

RTSP 认证

支持 **digest** 和 **digest/basic** 认证方式，表示向设备发送 RTSP 请求时需要携带认证信息，如果选择 **digest/basic** 认证方式，表示支持 **digest** 或 **basic** 认证，选择 **digest** 认证方式时，表示只支持 **digest** 认证。

RTSP 摘要算法

进行 RTSP 认证时，支持 MD5、SHA256 和 MD5/SHA256 加密算法。启用 MD5 之外的摘要算法后，第三方平台由于兼容性问题可能无法登录设备或预览。请考虑实际场景选择算法类型，建议优先采用高强度的加密算法。

WEB 认证

支持 **digest** 和 **digest/basic** 认证方式，表示向设备发送 WEB 请求时需要携带认证信息，如果选择 **digest/basic** 认证方式，表示支持 **digest** 或 **basic** 认证，选择 **digest** 认证方式时，表示只支持 **digest** 认证。

WEB 摘要算法

进行 WEB 认证时，支持 MD5、SHA256 和 MD5/SHA256 加密算法。启用 MD5 之外的摘要算法后，第三方平台由于兼容性问题可能无法登录设备或预览。请考虑实际场景选择算法类型，建议优先采用高强度的加密算法。



说明

协议要求携带的认证信息请参看具体协议内容。

9.13.2 SSH

建立在应用层基础上的安全协议，启用后可有效防止远程管理过程中的信息泄露问题。

单击 **配置** → **系统** → **安全管理** → **安全服务** 可控制 **启用 SSH**。

9.13.3 开启账户锁定

用于提升设备网络访问的安全性。

admin 用户可以设置密码错误尝试次数和锁定时间。当密码输入错误达到限定的次数，设备将自动锁定。达到设置的锁定时间后，设备自动解锁。

通过 **配置** → **系统** → **安全管理** → **安全服务**，勾选 **开启非法登录锁定**，设置 **错误尝试次数** 和 **锁定时间**。

9.13.4 控件超时配置

通过浏览器操作设备时，在设定的时间范围内，如果没有对设备进行任何操作（不包括查看实时图像），设备将自动注销，需重新登录。

通过 **配置** → **系统** → **安全管理** → **高级安全**，勾选 **启用控件超时**，设置 **超时时间**，单击 **保存**。

9.13.5 证书管理

用于创建、集中管理设备所有证书。

服务器/客户端证书



设备含默认安装的自签名证书，证书 ID 为 *default*。

创建自签名证书

操作步骤

1. 进入 **配置 → 系统 → 安全管理 → 证书管理**。
 2. 单击 **创建自签名证书**。
 3. 设置证书信息。
-



证书 ID 须唯一不可重复。

4. 单击 **确定**。

服务器端/客户端证书列表显示当前创建的自签名证书。

使用**功能列**可查看所有通过当前证书进行身份校验的协议类型。

5. 可选操作: 单击 **证书属性**，查看证书更多属性，如证书颁发机构等。

创建证书请求和安装证书

用于导入由设备生成证书请求，并经受信任机构签名的证书。

前提条件

已创建自签名证书。

操作步骤

1. 进入 **配置 → 系统 → 安全管理 → 证书管理**。
2. **服务器端/客户端证书**列表选择自签名证书。
3. 单击 **创建证书请求**。
4. 设置证书请求信息。
5. 单击 **确定**。

弹窗显示证书详情。上下滑动可查看全文。

6. 复制证书详情并将其存成本地的请求文件。
7. 将请求文件发送到证书认证机构进行签名。
8. 导入证书认证机构发送回的证书。
 - 1) 单击 **导入**。
 - 2) 设置证书 ID。

 说明

证书 ID 须唯一不可重复。

- 3) 单击 **浏览**，根据本地路径选择待导入的证书。
- 4) 选择 **自签名请求证书** 导入方式。
- 5) 单击 **确定**。

服务器端/客户端证书列表显示当前导入的证书。

使用功能列可查看所有通过当前证书进行身份校验的协议类型。

9. 可选操作: 单击 **证书属性**，查看证书更多属性，如证书颁发机构等。

安装第三方机构签名证书

用于导入由第三方机构进行认证的签名证书。

前提条件

已获取第三方机构签名证书。

操作步骤

1. 进入 **配置 → 系统 → 安全管理 → 证书管理**。
2. 单击 **导入**。
3. 设置证书 ID。

 说明

证书 ID 须唯一不可重复。

4. 单击 **浏览**，根据本地路径选择待导入的证书。
5. 选择 **证书和密钥** 导入方式。

独立私钥 适用于证书密钥存储在独立私钥文件的情况。

单击 **浏览**，根据本地路径选择待导入的证书文件和私钥文件并输入 **私钥密码**。

PKCS#12 适用于证书密钥和证书为同一个文件的情况。此时输入 **密码** 即可。

6. 单击 **确定**。

服务器端/客户端证书列表显示当前导入的证书。

使用功能列可查看所有通过当前证书进行身份校验的协议类型。

安装 CA 证书

用于导入由权威证书签证机关（CA）颁发的证书（一般权威的 CA 组织需要收费），提高访问的安全等级。

前提条件

已获取 CA 证书。

操作步骤

1. 进入 **配置 → 系统 → 安全管理 → 证书管理**。
2. 单击**导入**，根据本地路径选择待导入的 CA 证书。
3. 单击**确定**。

CA 证书列表显示当前导入的证书。

使用**功能列**可查看所有通过当前证书进行身份校验的协议类型。

证书过期报警

用于管理和监测设备证书的有效期，当发现证书有效期异常将进行联动报警。

通过 **配置 → 系统 → 安全管理 → 证书管理**，设置相关参数。

启用证书报警

表示开启设备对证书有效期的管理和监测。

过期前提醒

设置证书过期前几天进行报警提醒。例如：证书过期前提醒日期设置为 2 天，则设备将按照证书有效截止时间前 2 天开始提醒。

报警频率

设置证书有效期异常后，触发报警的频率。

报警检测时间

设置设备每日对证书有效期的检测时间，当检测到证书有效期异常将立即进行联动报警。

9.13.6 设置 HTTPS

网络访问中，要提高浏览器访问的安全性，可通过 HTTPS 协议构建安全、加密的网络传输，通过身份认证和加密通讯，保证传输数据的安全性。

操作步骤

1. 进入 **配置 → 网络 → 高级配置 → HTTPS**。
2. 勾选**启用**，通过 HTTPS 协议访问设备。
3. 可选操作: 勾选**自动跳转 HTTPS**，可将输入的 IP 地址自动转换成 HTTPS 地址，提升网络安全性。
4. 选择**服务端证书**。



通过 **配置 → 系统 → 安全管理 → 证书管理** 可查看设备各类证书。

5. 单击 **保存**。

9.13.7 安全审计日志

安全审计日志是指安全操作相关的日志。通过查询和分析设备内置存储中的安全日志，可排查非法入侵和安全事件引起的故障。由于存储空间有限，建议您设置日志服务器，将安全日志上传至日志服务器存储。



安全审计日志功能视型号而定，请以实际设备为准。

查询安全审计日志

用于查询和管理设备的安全日志。

操作步骤

1. 进入 **配置 → 系统 → 升级维护 → 安全审计日志**。
2. 设置日志类型、开始时间和结束时间。
3. 单击 **查找**。

日志列表中显示符合查询条件的所有日志信息。

4. 可选操作: 单击 **导出**，可将日志保存到计算机上。

配置安全审计日志服务器

用于将安全日志上传并存储至日志服务器。

前提条件

- 已获取到日志服务器的 IP 地址和端口。
- 设备已安装客户端证书或 CA 证书。通过 **配置 → 系统 → 安全管理 → 证书管理** 可查看设备各类证书。
- 若日志服务器端配置为双向认证，设备需同时选择客户端证书和 CA 证书；若日志服务器端配置为单向认证，则设备需只需选择 CA 证书。

操作步骤

1. 进入 **配置 → 系统 → 系统维护 → 安全审计日志**。
2. 设置日志上传服务器。
 - 1) 勾选 **启用日志上传服务器**。

- 2) 勾选**启用传输加密**，设备发往服务器的日志将会进行加密传输。



设备未选择客户端证书和 CA 证书时，加密传输不生效。

- 3) 设置日志服务器参数。

日志服务器地址

需要存储日志的服务器地址，如 IP 地址。

日志服务器端口

日志服务器的数据端口。

- 4) 可选操作: 选择**客户端证书**。

- 5) 选择**CA 证书**。

- 6) 单击**测试**，测试设备和服务器连接状态。

测试成功表示设备能够正常连接到日志服务器。

3. 单击**保存**。

结果说明

设备将定时上传安全审计日志到日志服务器。



功能视型号而定，请以实际界面为准。

9.13.8 设置 QoS

通过配置 QoS 参数，可有效解决网络延迟和网络阻塞问题。



QoS 功能需要传输路径上的网络设备（如路由器、交换机等）支持。

操作步骤

1. 进入 **配置 → 网络 → 高级配置 → QoS**。

2. 根据 QoS 分类标准，设置**视/音频 DSCP**、**报警 DSCP** 和**管理 DSCP** 参数。



网络可根据 DSCP 权值来判断数据传输的优先级。DSCP 值越大，优先级越高，配置时需要在路由器端设置相同的值。

3. 单击**保存**。
-

9.14 管理设备用户

介绍如何管理设备用户。

9.14.1 设置用户账户和权限

介绍设备用户添加、修改、删除和用户权限分配。



注意

为了提高产品网络使用的安全性，请您定期更改用户名的密码，建议每 3 个月进行 1 次更新维护。如果设备在较高安全风险的环境中使用，建议每月或每周进行 1 次更新。

操作步骤

1. 进入 **配置** → **系统** → **用户管理** → **用户管理**。
2. 单击**添加**，设置**用户名**，**用户类型**和**密码**，根据使用需求分配用户远程权限。

管理员

管理员拥有一切操作权限，可以添加普通用户和操作员，并对添加的用户分配权限。

普通用户

只能查看实况、配置云台参数和修改自己的密码，无其他操作权限。

操作员

拥有除对管理员的操作权限，无创建用户的权限。

选择用户，单击**修改** 修改所选用户的密码、权限等信息。

选择用户，单击**删除** 删除所选用户。



说明

- 管理员最多可创建 31 个用户。
- 密码长度小于 8 位、密码只包含一类字符，密码与用户名相同，密码是用户名的倒转输入，密码包含用户名，密码包含倒转输入的用户名，以上几类密码属于风险密码，为更好保护您的隐私并提升产品安全性，建议您将风险密码更改为高强度密码。
- 密码强度规则如下：
 - 强密码：包含三种或三种以上类型（如数字、小写字母、大写字母、特殊字符）组合的密码。
 - 中密码：由数字和特殊字符、小写字母和特殊字符、大写字母和特殊字符、小写字母和大写字母组合的密码。
 - 弱密码：由数字和小写字母组合、数字和大写字母组合的密码。

3. 单击**确定**。

9.14.2 查看在线用户

用于显示网络中登录到设备上的用户列表。

通过 **配置 → 系统 → 用户管理 → 在线用户**，查看访问过设备的用户列表。

9.14.3 设备同时登录数

介绍设备同时登录数的设置。

登录管理员（admin）用户，选择 **配置 → 系统 → 用户管理**，单击**通用参数**，可设置同时登录设备的路数。



杭州海康威视数字技术股份有限公司
HANGZHOU HIKVISION DIGITAL TECHNOLOGY CO., LTD.

www.hikvision.com
服务热线: 400-800-5998

UD27140B