

网络硬盘录像机

快速操作手册













V1.1.0

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。

变更记录

版本号	修订内容	发布日期
V1.1.0	<ul style="list-style-type: none">设备初始化页面更新。“P2P设置”改为“乐橙云设置”。添加远程设备页面更新。	2020.12
V1.0.0	首次发布。	2019.06

使用安全须知

下面是关于产品的正确使用方法、为预防危险、防止财产受到损失等内容，使用设备前请仔细阅读本说明书并在使用时严格遵守，阅读后请妥善保存说明书。

使用要求

- 请勿将设备放置和安装在阳光直射的地方或发热设备附近。
- 请勿将设备安装在潮湿、有灰尘或煤烟的场所。
- 请保持设备的水平安装，或将设备安装在稳定场所，注意防止本产品坠落。
- 请勿将液体滴到或溅到设备，并确保设备上没有放置装满液体的物品，防止液体流入设备。
- 请将设备安装在通风良好的场所，切勿堵塞设备的通风口。
- 仅可在额定输入输出范围内使用设备。
- 请勿随意拆卸设备。
- 请在允许的湿度和温度范围内运输、使用和存储设备。

电源要求

- 请务必按照要求使用电池，否则可能导致电池起火、爆炸或燃烧的危险。
- 更换电池时只能使用同样类型的电池。
- 产品必须使用本地区推荐使用的电线组件（电源线），并在其额定规格内使用。
- 请务必使用设备标配的电源适配器，否则引起的人员伤害或设备损害由使用方自己承担。
- 请使用满足SELV（安全超低电压）要求的电源，并按照GB8898（IEC60065）或GB4943.1（IEC60950-1符合Limited Power Source（受限制电源））的额定电压供电，具体供电要求以设备标签为准。
- 请将I类结构的产品连接到带保护接地连接的电网电源输出插座上。
- 器具耦合器为断开装置，正常使用时请保持方便操作的角度。

目录

前言	I
使用安全须知	II
第 1 章 安装设备	1
1.1 开箱检查	1
1.2 安装硬盘	1
1.2.1 1.5U和2U机箱示例	2
1.2.2 3U机箱示例	5
第 2 章 设备结构	7
2.1 前面板	7
2.2 后面板	7
第 3 章 设备连接	10
第 4 章 本地基本操作	11
4.1 开机	11
4.2 设备初始化	11
4.3 重置密码	14
4.4 开机向导	16
4.5 一键添加IPC	17
4.6 添加远程设备	18
4.7 设置录像计划	18
4.8 即时回放	19
第 5 章 WEB操作	21
第 6 章 乐橙云设置	22
附录1 法律声明	23
附录2 网络安全建议	24

第 1 章 安装设备



注意

设备不支持壁挂安装。

1.1 开箱检查

运输公司将您所需的硬盘录像机送到您手中时，请对照下表进行开箱检查，若有任何问题，请及时联系公司的售后服务人员。

检查顺序	检查项	检查内容	
1	整体包装	外观	有无明显的损坏
		包装	有无意外撞击
		配件（保修卡上的配件清单）	是否齐全
2	标签	机身上贴的标签	设备型号是否与订货合同一致 标签有无撕毁  说明 不要撕毁、丢弃，否则不保证提供保修服务。 在您拨打公司的售后服务电话时，需要您提供该标签上的产品序列号。
3	机壳	外观	有无明显的损坏
		前面板的数据线、电源线、风扇电源和主板	连接是否松动  说明 若有松动，请及时联系公司的售后服务人员。

1.2 安装硬盘

初次安装时先检查是否已安装硬盘，推荐使用企业级或监控级硬盘，不建议使用PC硬盘。



注意

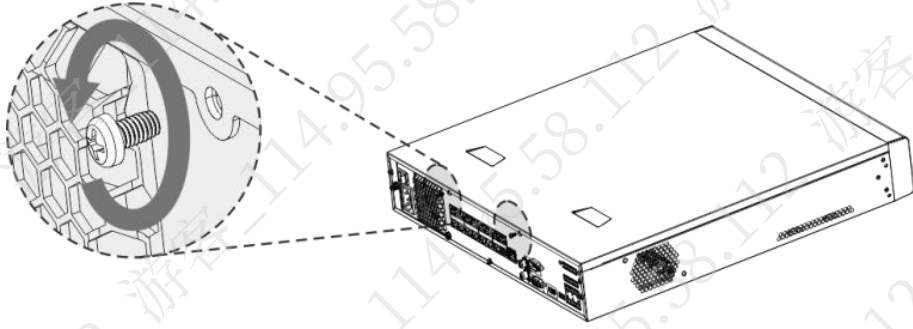
安装硬盘前，请先切断电源后再打开机箱。

1.2.1 1.5U和2U机箱示例

不同设备型号需要安装的硬盘数量不同，请以实际为准。

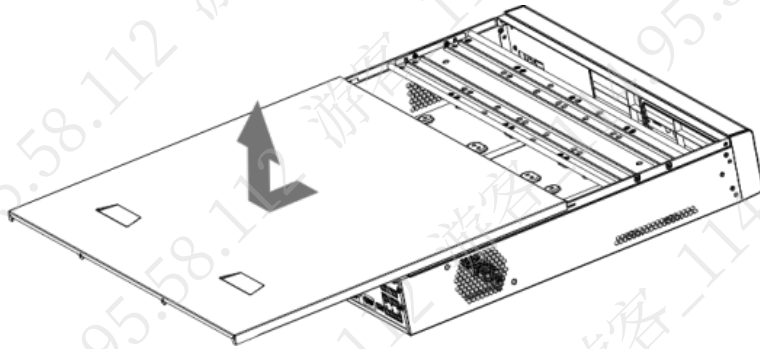
步骤1 拆卸设备后面板上的固定螺钉。

图1-1 拆卸固定螺钉



步骤2 沿图1-2中箭头所示方向取下机箱盖。

图1-2 取下机箱盖



步骤3 拆卸硬盘支架边上的螺钉，取下硬盘支架。

- 4盘位设备具有一个硬盘支架，拆卸方式如图1-3所示。
- 8盘位设备具有两个硬盘支架，拆卸方式如图1-4所示。

图1-3 拆卸硬盘支架（4盘位设备）

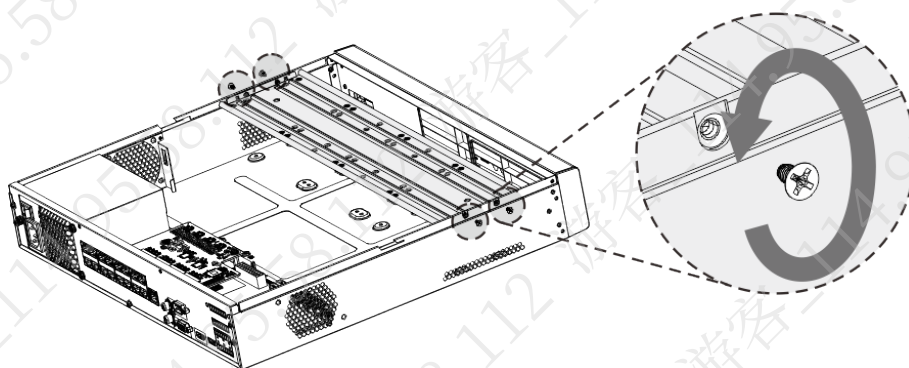
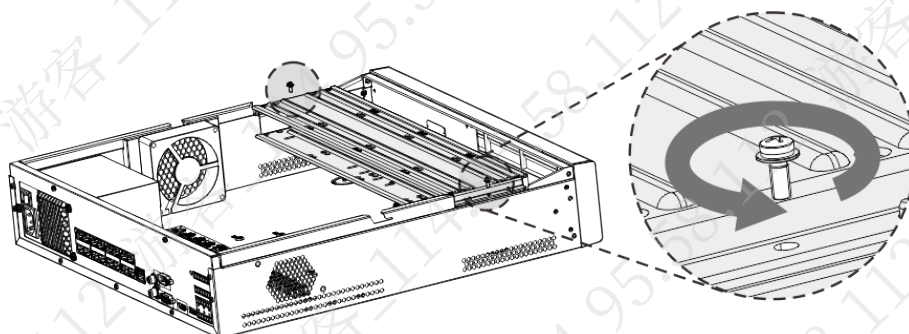
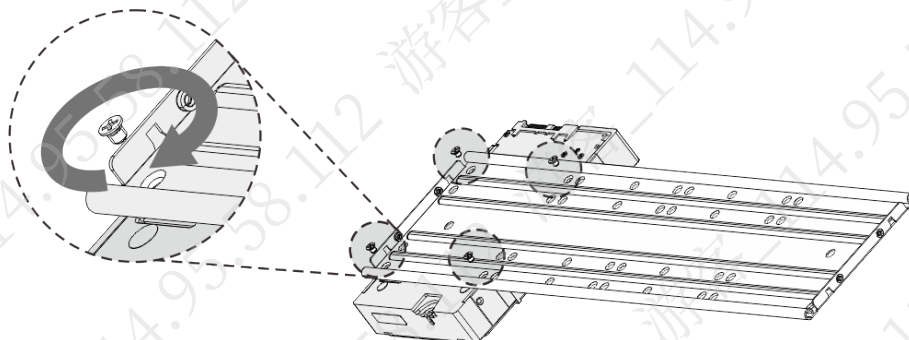


图1-4 拆卸硬盘支架（8盘位设备）



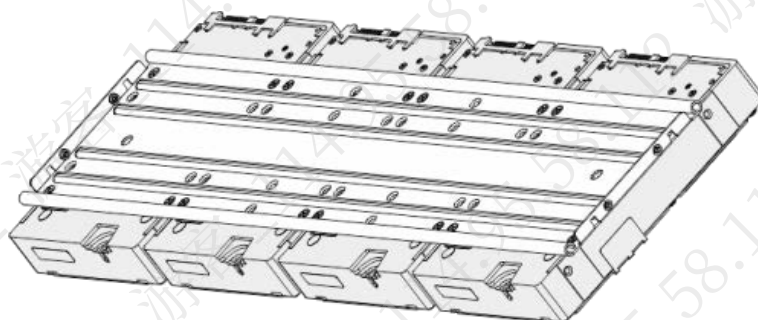
步骤4 将硬盘上的4个螺丝孔对准硬盘架上的4个螺丝孔，锁紧螺钉，将硬盘固定至硬盘架上。

图1-5 锁定硬盘（1）



步骤5 参考步骤4，依次安装其他硬盘。

图1-6 锁定硬盘（2）



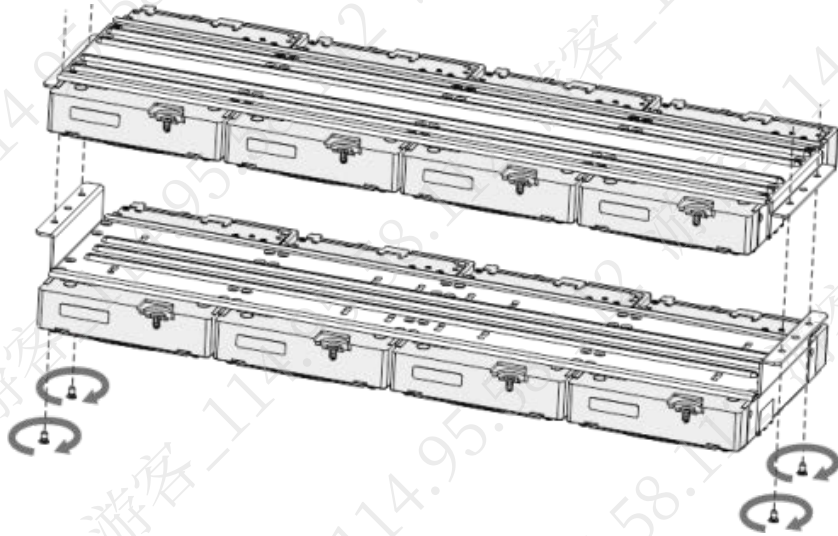
步骤6 锁定两个硬盘支架。



说明

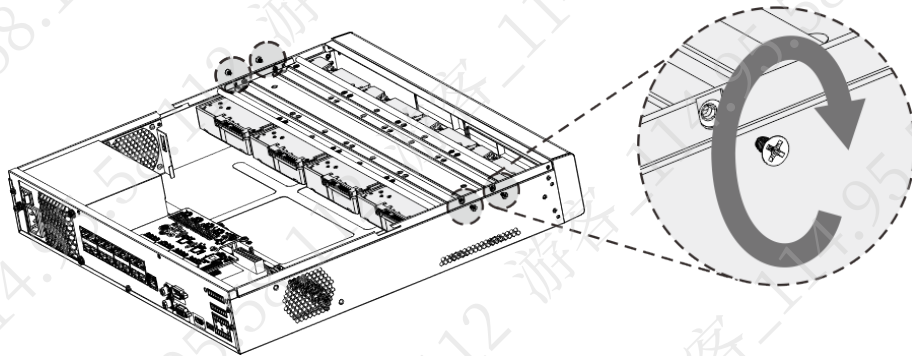
仅8盘位设备需要执行此步骤。

图1-7 锁定两个硬盘支架



步骤7 将硬盘支架放置至设备上，并锁定硬盘支架边上的螺钉。

图1-8 锁定硬盘支架



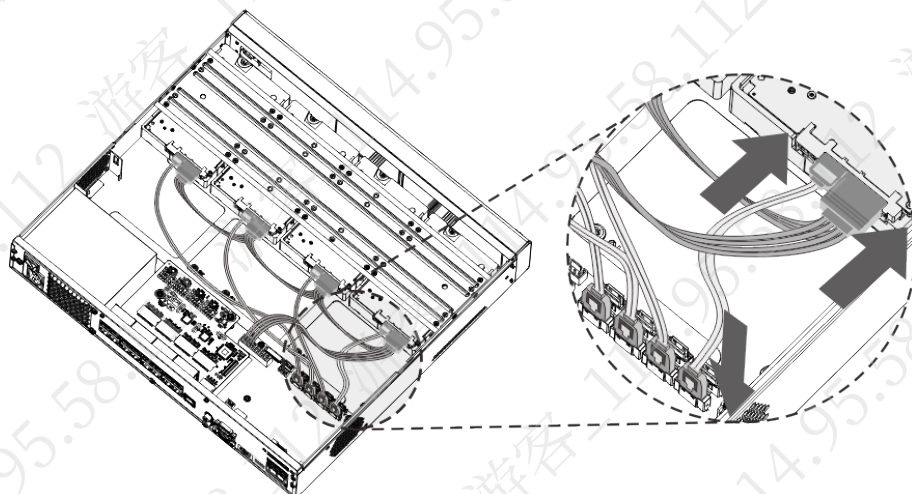
步骤8 连接硬盘和设备的数据线和电源线。



说明

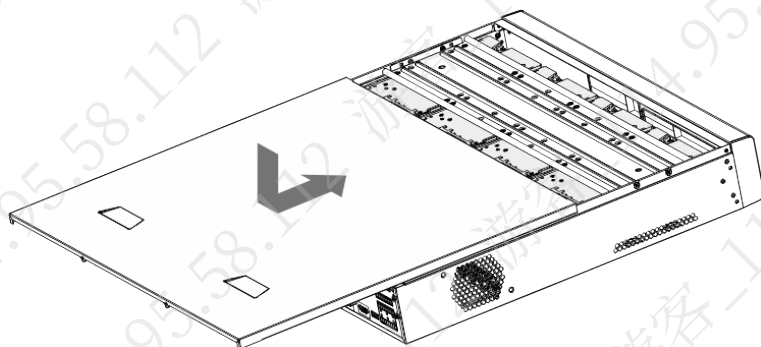
图1-9中的接线连接4块硬盘为例，请以实际设备的盘位为准。

图1-9 连接线缆



步骤9 合上机箱盖，并锁定设备后面板的2个固定螺钉，完成安装。

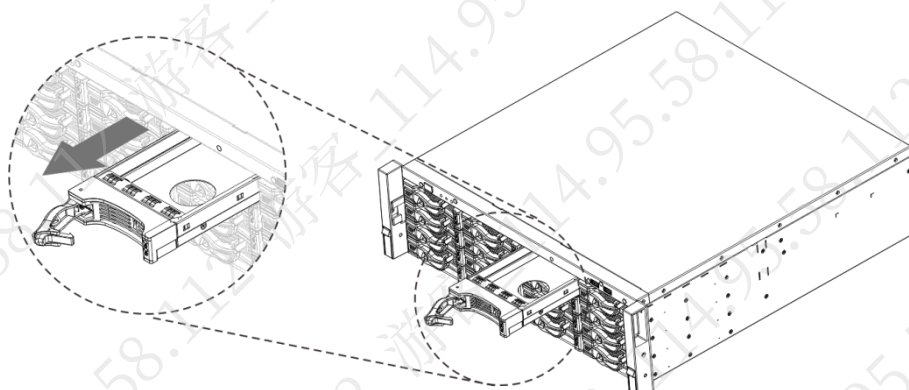
图1-10 完成安装



1.2.2 3U机箱示例

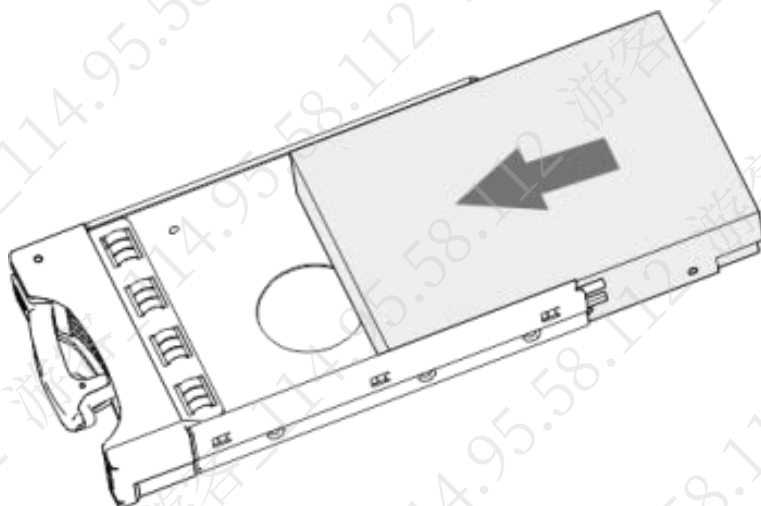
步骤1 按设备前面板硬盘盒上的按钮，打开把手并向外拉动，取出硬盘盒。

图1-11 取出硬盘盒



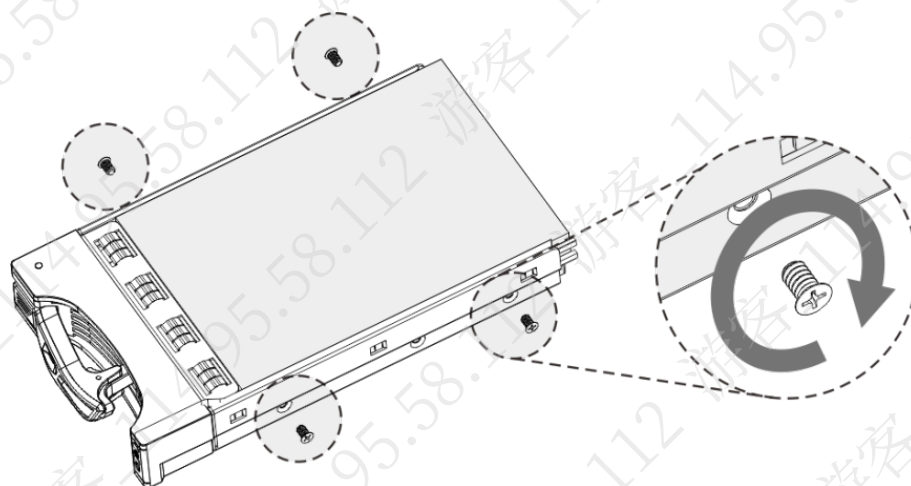
步骤2 沿图1-12中箭头所示方向，将硬盘插入硬盘盒中。

图1-12 插入硬盘



步骤3 锁定硬盘盒两侧的螺钉。

图1-13 锁定螺钉



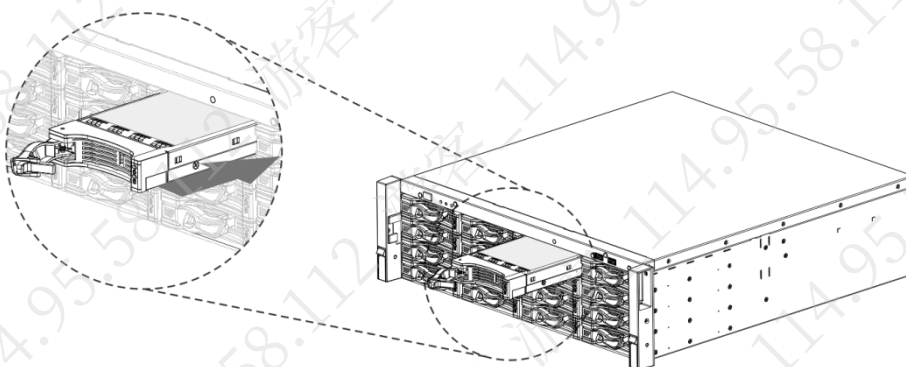
步骤4 将硬盘盒插入硬盘插槽，推到底并合上硬盘盒把手。



说明

插入硬盘盒时，如果硬盘盒未推到底，请勿合上把手，以免硬盘插槽损坏。

图1-14 插入硬盘盒



第 2 章 设备结构

以下内容以NVR44-16P-4KS2系列为例，其他型号设备请参见使用说明书。

2.1 前面板

图2-1 前面板示意图

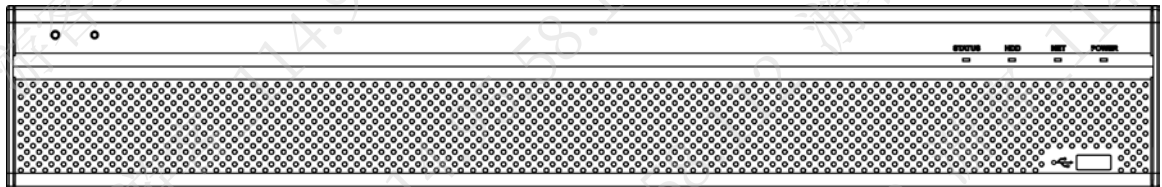



表2-1 前面板功能介绍表

标识	名称	功能
STATUS	状态指示灯	设备启动后，蓝灯常亮。
HDD	硬盘状态指示灯	<ul style="list-style-type: none">硬盘正常时，不亮。硬盘异常时，蓝灯常亮。
NET	网络状态指示灯	<ul style="list-style-type: none">网络连接正常时，不亮。网络连接异常时，蓝灯常亮。
POWER	电源状态指示灯	电源连接正常时，蓝灯常亮。
	USB接口	外接USB存储设备、鼠标、刻录光驱等。

2.2 后面板

图2-2 后面板示意图

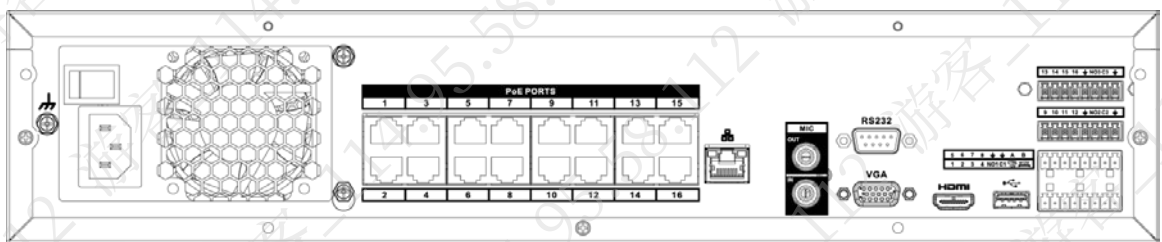






表2-2 后面板功能介绍表

标识	接口名称	接口功能
	电源开关	电源开关。
	电源输入接口	电源接口，输入AC 220V交流电。
MIC IN	音频输入接口	语音对讲输入接口，接收来自话筒、拾音器等设备输出的模拟音频信号。

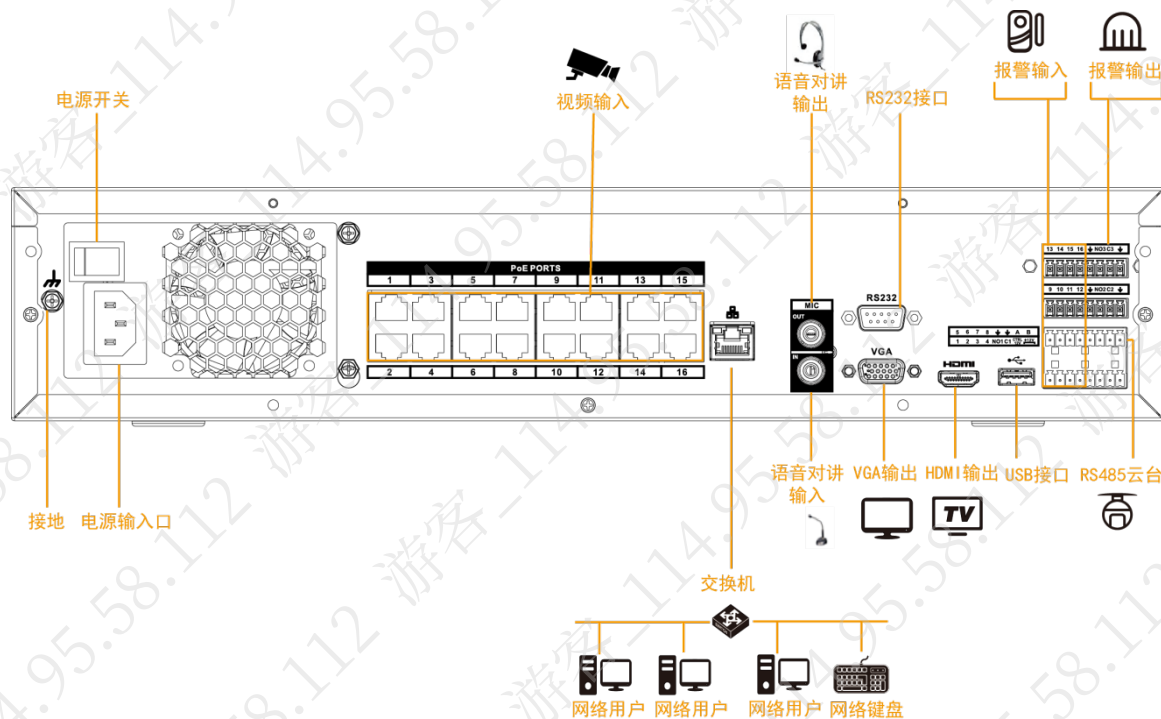
标识	接口名称	接口功能
MIC OUT	音频输出接口	<p>音频输出接口，输出模拟音频信号给音箱等设备。</p> <ul style="list-style-type: none"> • 语音对讲输出 • 单画面视频监控声音输出 • 单画面视频回放声音输出
VIDEO OUT	视频输出接口	使用CVBS方式输出。
1~16	报警输入端口1~16	<ul style="list-style-type: none"> • 4组报警输入接口（组1：端口1~4，组2：端口5~8，组3：9~12，组4：13~16），接收外部报警源的开关量信号，可以为常开型或常闭型报警输入。 • 当用外部电源对报警输入设备供电时，报警输入设备需要与NVR设备共地。 <p> 说明 NVR44-4KS2/44-HDS2系列，可选8进2出的报警。</p>
	接地端	报警输入接地端。
NO1~NO3	报警输出端口1~3	<ul style="list-style-type: none"> • 3组报警输出接口（组1：端口NO1~C1，组2：端口NO2~C2，组3：端口NO3~C3），输出报警信号给外部报警设备，外部报警设备需有电源供电。 • NO：常开型报警输出端。 • C：报警输出公共端。 <p> 说明 NVR44-4KS2/44-HDS2系列，可选8进2出的报警。</p>
C1~C3		<ul style="list-style-type: none"> • 3组报警输出接口（组1：端口NO1~C1，组2：端口NO2~C2，组3：端口NO3~C3），输出报警信号给外部报警设备，外部报警设备需有电源供电。 • NO：常开型报警输出端。 • C：报警输出公共端。 <p> 说明 NVR44-4KS2/44-HDS2系列，可选8进2出的报警。</p>

标识	接口名称	接口功能
A	RS485通信接口	RS485_A接口，控制485设备的A线，用于连接如外部球机云台等设备。
B		RS485_B接口，控制485设备的B线，用于连接如外部球机云台等设备。
CTRL 12V	-	可控12V电源输出，控制开关量报警继电器的输出，利用12V电压的有、无控制报警设备报警。同时也可作为某些报警设备如报警探测器的电源输入。
+12V		+12V电源输出接口，给外部设备如摄像机、报警设备供电，要求外接的设备电源在1A以下。
	网络接口	10/100/1000Mbps自适应以太网接口，连接网线。
eSATA	eSATA接口	SATA的外接式接口，可外接SATA接口的设备，当外接硬盘时，硬盘需要做相应的跳线处理。
	USB接口	USB接口，连接鼠标、USB存储设备、刻录光驱等。
RS232	RS232透明调试串口	用于普通串口调试，配置IP地址，传输透明串口数据。
HDMI	高清晰多媒体接口	高清音、视频信号输出接口，传输未经压缩的高清视频和多声道音频数据给具有HDMI接口的显示设备。HDMI版本号是1.4。
VGA	VGA视频输出接口	VGA视频输出接口，输出模拟视频信号，可连接监视器观看模拟视频输出。
	接地端	接地孔。

第 3 章 设备连接

以下内容以NVR44-16P-4KS2系列为例，其他型号设备请参见使用说明书。

图3-1 设备连接图



第 4 章 本地基本操作



说明

不同型号设备界面可能存在差异，以下截图仅供参考，请以实际界面显示为准。

4.1 开机



注意

- 检查供电的输入电压与设备电源是否对应，确认与电源线接好后，再打开电源开关。
- 为保护设备，请先将设备与电源适配器连接，再接通电源。
- 为保证设备和外接设备（如摄像机）稳定工作、延长硬盘使用寿命，建议您参考国际标准提供电压值稳定、波纹干扰小的电源输入。推荐使用UPS电源。

连接设备和显示器，插入电源后，按设备的电源开关键，即可开启设备。

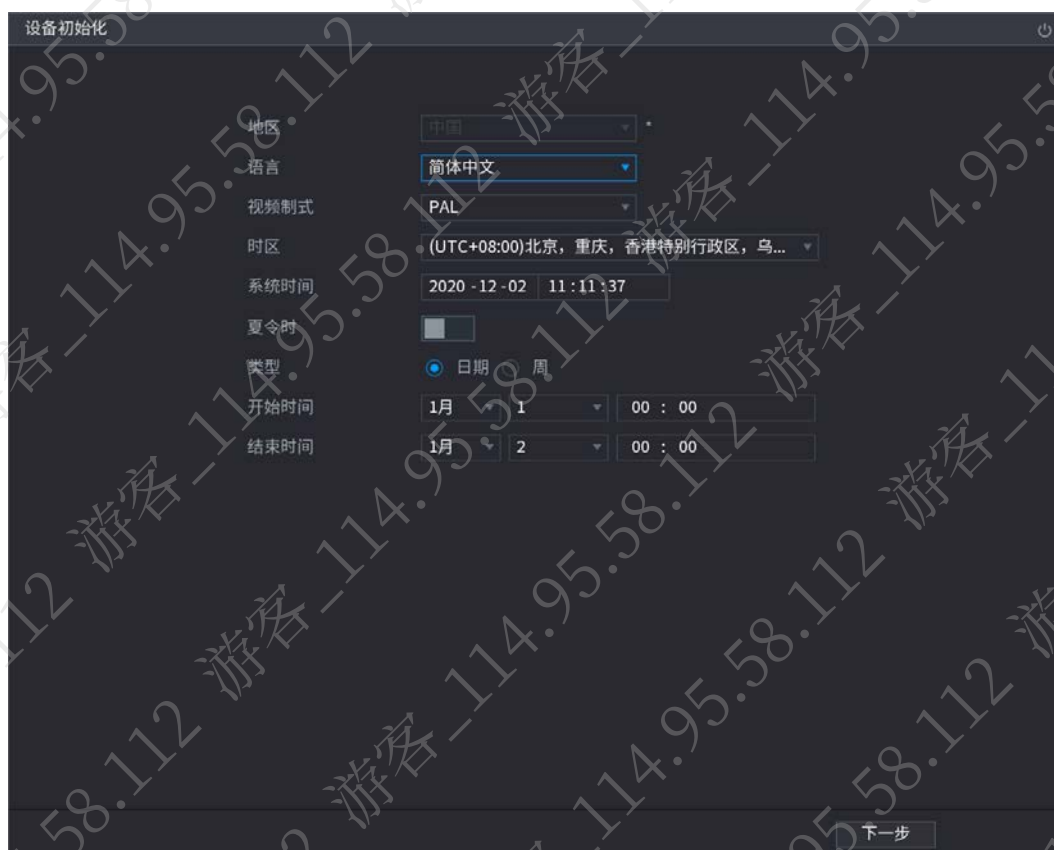
4.2 设备初始化

首次开机时，需要设置设备管理员用户名和密码（管理员用户名默认为admin）。为确保设备安全，请您妥善保存admin的登录密码，并定期修改。

步骤1 开启设备。

步骤2 根据实际情况设置地区、时区、系统时间等基本信息，单击“下一步”。

图4-1 设备初始化



步骤3 设置admin的登录密码。

图4-2 密码设置



步骤4 设置“密码”、“密码确认”和“密码提示”，并单击“下一步”。

密码可设置为8位~32位非空字符，可以由字母、数字和特殊字符（除“!”、“”、“;”、

“:”、“&”外)组成。密码必须由其中的2种或2种以上字符组成, 请根据密码强弱提示设置高安全性密码。

步骤5 设置手势密码或者单击“跳过”。



说明

设置手势密码后, 系统默认使用手势密码登录。如果未设置手势密码, 则需要输入密码进行登录。

图4-3 密码保护

步骤6 设置密码保护, 详细介绍请参见表4-1。



说明

- 设置密码保护后, 如果您遗忘了admin的登录密码, 可以通过预留手机或者密保问题重置admin的密码。重置密码的详细操作请参见设备对应的使用说明书。
- 如果不需要设置密码保护, 可取消选择“预留手机”和“密保问题”。

表4-1 密码保护说明

密码保护方式	说明
预留手机	设置预留手机号码。重置密码时, 扫描二维码, 输入预留手机接收到的安全码后即可重置admin密码。
密保问题	设置密保问题和答案。重置密码时, 正确回答密保问题即可重置admin密码。


步骤7 单击“确定”, 完成设备初始化。

系统显示开机向导界面, 详细操作请参见“4.4 开机向导”。

4.3 重置密码

当您遗忘admin用户的登录密码时，可以通过如下方式重置密码。

- 密码重置功能开启时，可通过手机扫描本地界面二维码进行密码重置。
- 密码重置功能关闭时，可通过之前配置的“密保问题”来找回密码。若之前未配置“密保问题”，则系统直接提示“密码重置已关闭！”，如需重置密码，请联系技术客服。

步骤1 单击登录界面的。



说明


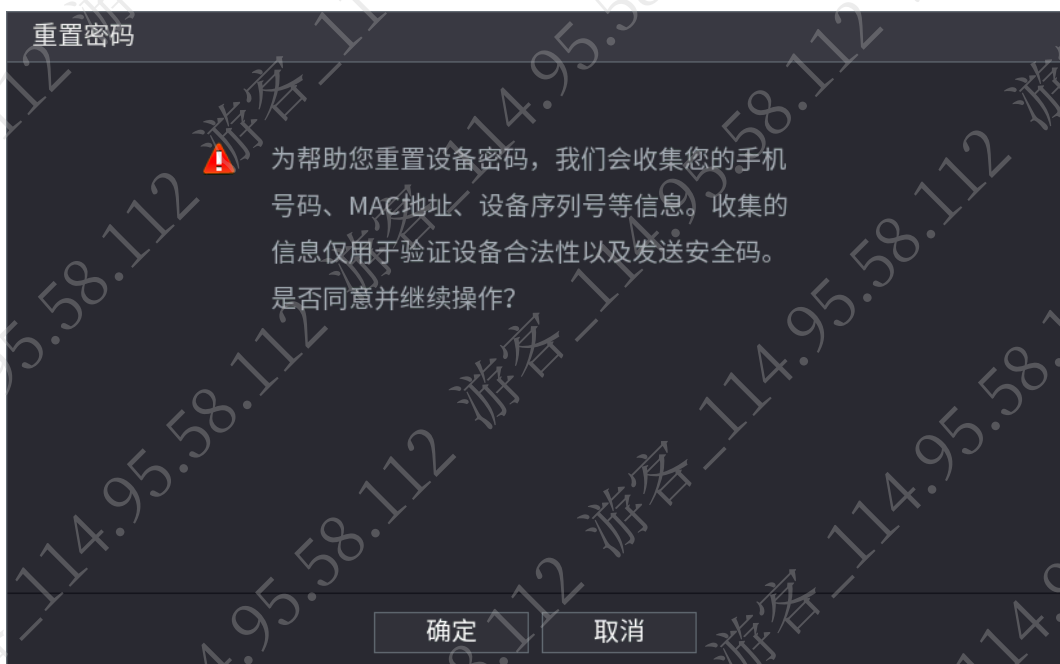
- 如果是手势密码登录界面，请单击“忘记手势”，切换为密码登录界面后，单击。
- 未设置预留手机时，系统显示设置预留手机界面。设置预留手机后，单击“下一步”。

图4-4 重置密码（1）



步骤2 单击“确定”。



说明

单击“确定”后，我们会收集您的手机号码、MAC地址、设备序列号等信息，收集的信息仅用于验证设备合法性以及发送安全码。请仔细阅读提示并确定是否同意信息收集操作。

图4-5 重置密码（2）

步骤3 重置登录密码。

- 手机找回

根据界面提示扫描二维码并获取安全码，在“请输入安全码”文本框中输入预留手机接收到的安全码。



说明

- ◇ 扫描同一个二维码最多可获取两次安全码，如需再次获取安全码，请刷新二维码扫描界面。
- ◇ 预留手机接收到安全码后，请在24小时内使用安全码重置密码，否则安全码将失效。
- 密保问题
单击“找回方式”的下拉框，选择“密保问题”，系统显示密保问题界面。选择问题并在“答案”文本框中正确输入预先设置的密保问题答案。

图4-6 重置密码 (3)



The screenshot shows a '重置密码' (Reset Password) screen. At the top, there are two radio buttons for '找回方式' (Recovery Method): '密保问题' (Security Questions) is selected. Below this, there are three security questions, each with a corresponding answer input field. The questions are: '你小时候最喜欢哪一本书?' (Which book did you like best in your childhood?), '你第一个上司姓什么?' (What is the surname of your first supervisor?), and '你最喜欢的水果是什么?' (What is your favorite fruit?). At the bottom of the screen, there are two buttons: '下一步' (Next Step) and '取消' (Cancel).

步骤4 单击“下一步”，重新设置“新密码”和“确认密码”。



说明

密码可设置为8位~32位非空字符，可以由字母、数字和特殊字符（除“”、“”、“;”、“:”、“&”外）组成。密码必须由其中的2种或2种以上字符组成，请根据密码强弱提示设置高安全性密码。

步骤5 单击“确定”，完成密码重置。

4.4 开机向导



说明

如果首次开启设备时已配置完“开机向导”的所有配置项，则下次开机后系统将不再出现“开机向导”界面。

单击“下一步”，登录后即可进入开机向导界面，可快速配置设备，详细介绍请参见使用说明书。

- 选择“开启一键添加功能”时，登录后，设备自动搜索并添加同一个局域网的远程设备，详细介绍请参见“4.5 一键添加IPC”。
- 选择“自动检测”，则系统每天自动检测更新程序。

图4-7 开机向导

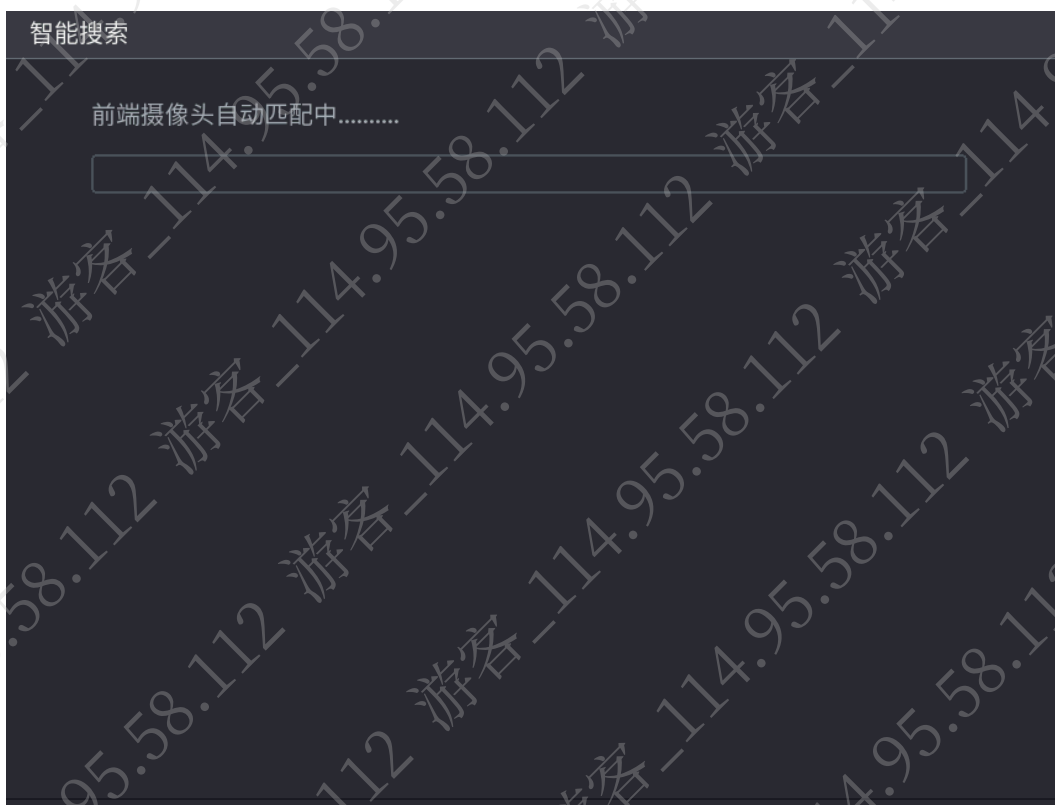


4.5 一键添加IPC

在“开机向导”中选择“开启一键添加功能”，或者在预览界面右键选择“一键添加”。

当IPC和NVR接入同一个交换机或路由器时，通过一键添加，可以快速将IPC添加到NVR的通道中。

图4-8 一键添加



4.6 添加远程设备

选择“主菜单 > 摄像头 > 远程设备”。

您可以通过以下方式添加远程设备：

- 单击“设备搜索”，在搜索列表中双击远程设备或者选择远程设备前的复选框后单击“添加”。
- 单击“手动添加”，输入远程设备的IP地址进行添加。

图4-9 远程设备



4.7 设置录像计划

设备出厂默认录像模式是各通道24小时连续录像，您可以根据需要设置录像时间和录像类型。

步骤1 选择“主菜单 > 存储 > 存储计划”。


图4-10 录像设置



步骤2 设置通道、预录时间、断网续传、录像类型等。

- 在NVR上设置某块硬盘为冗余盘后，可选择“冗余”，实现录像文件双备份功能，即将某通道的录像同时保存到不同硬盘上。当其中一个硬盘损坏时，在另一个盘上仍有备份文件，保证了数据的可靠性。
- 选择“断网续传”后的复选框，开启断网续传功能。当NVR检测到与IPC的网络连接中断时，IPC继续录像并存放在SD卡中，网络恢复后，IPC将断网期间的录像传回NVR，保证录像的完整性。

步骤3 设置录像计划时间段，包括绘图法和编辑法。

- 绘图法：按住鼠标左键，在时间段示意图中拖动鼠标绘制时间段。
- 编辑法：单击 ，设置录像时间段，并单击“确定”。

步骤4 单击“应用”，保存录像计划设置。

说明

开启自动录像功能后，配置的录像计划才会生效。开启自动录像的详细操作请参见设备对应的使用说明书。

4.8 即时回放


在预览界面，移动鼠标至通道画面上方中间区域内，单击控制条中的 ，系统开始回放当前通道前5分钟~60分钟的录像。

图4-11 控制条



第 5 章 WEB操作

首次登录设备时，需要执行设备初始化配置，详细操作请参见设备对应的使用说明书。

步骤1 打开浏览器，在地址栏中输入设备的IP地址，按【Enter】键。

图5-1 WEB登录界面



步骤2 输入“用户名”和“密码”。



说明

- 设备默认管理员用户名为admin，密码为首次设备初始化时设置的登录密码。为确保安全，建议您定期更改管理员密码，并妥善保存。
- 如果您遗忘了admin的登录密码，可在本地进行重置，重置密码的详细操作请参见设备对应的使用说明书。

步骤3 单击“登录”。

在WEB界面，可以进行系统配置、设备管理、网络配置等操作，详细介绍请参见设备对应的使用说明书。



说明

首次登录WEB时，请单击“请安装控件包”，安装控件包。

第 6 章 乐橙云设置

- 步骤1** 使用手机扫描手机客户端二维码，下载并安装手机客户端。
登录本地界面，选择“主菜单 > 网络设置 > 乐橙云设置”，或者登录WEB界面，选择“维护 > 网络设置 > 乐橙云设置”，获取手机客户端二维码和设备序列号二维码。
- 步骤2** 在手机客户端中添加设备。
设备添加成功后，即可在手机客户端上查看设备的监控画面。详细介绍请参见手机客户端配套的使用说明书。

附录1 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

- 本文档供多个型号产品使用，产品外观和功能请以实物为准。
- 如果不按照本文档中的指导进行操作而造成的任何损失由使用方自己承担。
- 本文档会实时根据相关地区的法律法规更新内容，具体请参见产品的纸质、电子光盘、二维码或官网，如果纸质与电子档内容不一致，请以电子档为准。
- 本公司保留随时修改本文中任何信息的权利，修改的内容将会在本文档的新版本中加入，恕不另行通知。
- 本文档可能包含技术上不准确的地方、或与产品功能及操作不相符的地方、或印刷错误，以公司最终解释为准。
- 如果获取到的PDF文档无法打开，请使用最新版本或最主流的阅读工具。

附录2 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。
- 不包含账户名称或账户名称的倒序。
- 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. 开启账户锁定

出厂默认开启账户锁定功能，建议您保持开启状态，以保护账户安全。在攻击者多次密码尝试失败后，其对应账户及源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. MAC地址绑定

请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。

8. 合理分配账户及权限

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。

9. 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。

10. 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。

11. 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。

12. 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。

13. 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。
- **开启设备IP/MAC地址过滤功能**, 限制允许访问设备的主机范围。