



SmartPSS Plus运维中心方案











使用说明书



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
V1.0.1	增加三方设备管理功能	2021.06
V1.0.0	首次发布	2021.03

目 录




前言	I
第 1 章 简介	1
第 2 章 打开运维中心方案	2
第 3 章 主界面介绍	3
第 4 章 设备管理	5
4.1 查看和配置设备信息	5
4.2 查看端口信息	6
4.3 配置端口信息	6
4.4 三方设备管理	8
4.5 处理报警	10
第 5 章 查询运维记录	11
附录1 法律声明	12
附录2 网络安全建议	14


第 1 章 简介

运维中心方案实现网络中设备状态实时监控，事件报警，支持远程重启设备，清理配置，恢复默认等操作。

第 2 章 打开运维中心方案

不同场景打开运维中心方案的操作方法不同。

- 如果是首次安装使用平台，在平台初始化过程中选择运维中心方案。登录后，在主页的左侧导航栏单击 ，打开方案。
- 如果已初始化平台，但未选择运维中心方案，在界面右上角选择“ > 切换方案”，选择运维中心方案。登录后，在主页的左侧导航栏单击 ，打开方案。

关于加载方案的详细介绍请参见平台使用说明书。在界面右上角选择“ > 帮助手册”，获取平台使用说明书。

第 3 章 主界面介绍

打开运维中心方案，选择“网络运维”进入方案主界面。

图3-1 网络拓扑

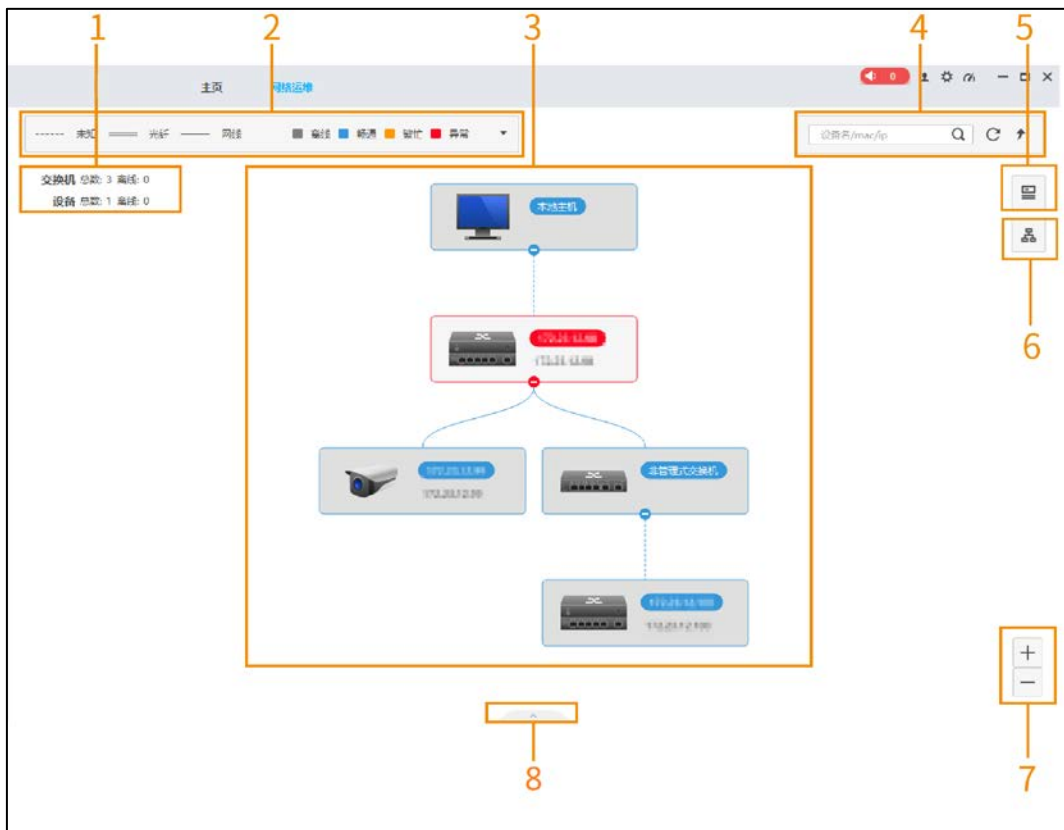










表3-1 主界面介绍

序号	功能	说明
1	设备数量	显示当前网络中存在的交换机及设备总数量和离线数量。
2	网络拓扑图标识	网络拓扑图的线缆类型及设备状态类型。单击展开设备类型。

序号	功能	说明
3	网络拓扑图	<p>当前网络拓扑结构。</p> <ul style="list-style-type: none"> 查看设备信息：双击设备或右键单击设备选择“设备详细信息”。部分设备支持在线设备管理，详细介绍请参见“4.1 查看和配置设备信息”。 查看链路详情：将光标停留到链路上，显示该链路的端口信息、传输速率（未知链路不支持查看）。 隐藏/显示子节点：单击/或右键单击设备选择“隐藏子节点”/“显示子节点”，将隐藏/显示该节点下连接的设备。 设为根节点（仅管理式交换机支持）：右键单击设备，选择“设为根节点”，拓扑图将以此设备为根节点重新排列。 删除离线节点（仅离线设备支持）：右键单击设备，选择“删除离线节点”，拓扑图中删除该节点。 处理报警：当设备状态为异常（红色）时，可选择处理报警。详细介绍请参见“4.5 处理报警”。
4	搜索设备、刷新、导出拓扑图、导出设备列表	<ul style="list-style-type: none"> 输入设备名、设备MAC地址或设备IP，在当前拓扑图中模糊搜索该设备。 单击，刷新拓扑图。 单击，导出当前拓扑图或设备列表。
5	三方设备管理	添加管理第三方设备，详细介绍请参见“4.4 三方设备管理”。
6	拓扑图显示设置	<ul style="list-style-type: none"> 设置拓扑图的显示层级。 选择网络摄像机及其任意一个管理交换机父节点，显示网络交换机与管理交换机之间的链路拓扑。
7	放大、缩小拓扑图	<ul style="list-style-type: none"> ：放大拓扑图。 ：缩小拓扑图。 <p>您也可以滑动鼠标滚轮调节拓扑图大小。</p>
8	实时事件列表	<ul style="list-style-type: none"> ：展开当前网络拓扑中实时事件列表。 ：收起当前网络拓扑中实时事件列表。

第 4 章 设备管理



4.1 查看和配置设备信息

在主界面，双击设备或右键单击设备选择“设备详细信息”，单击“设备信息”页签，查看设备详细信息。交换机设备支持重启设备、恢复默认配置、恢复出厂设置，配置设备告警等功能。

图4-1 设备信息



表4-1 设备配置参数

参数	说明
重启设备	单击“重启设备”，远程重新启动设备。
环路报警	启用后，当检测到同一设备的两个端口直连时产生报警。  说明 仅部分设备支持。
IP冲突	启用后，当检测到端口IP与当前网络中其他设备IP相同时产生报警。  说明 仅部分设备支持。
端口拥塞	启用后，当所有端口的使用量总和超过设置阈值时产生报警。
恢复默认参数	除网络参数、用户登录参数外，其他参数都恢复为出厂设置。

参数	说明
恢复设备出厂	将所有参数恢复为出厂设置，恢复后需重新初始化设备。

4.2 查看端口信息

支持查看管理式交换机端口信息，消除端口告警等功能。

在主界面，双击设备或右键单击设备选择“设备详细信息”，单击“端口信息”页签，选择端口。

- 端口详情：查看端口基本信息及报文统计信息。单击“清除”，清除该端口的所有统计信息。

图4-2 端口信息



- 报警详情：查看端口报警事件信息。
 - ◇ 单击操作列的 ，消除此条报警事件。
 - ◇ 选择多条报警事件，单击“批量报警消除”，消除多条报警事件。

4.3 配置端口信息

支持开启或关闭端口PoE状态、PD保活和端口远距离传输。

步骤1 在主界面，双击设备或右键单击设备选择“设备详细信息”。

步骤2 单击“端口配置”页签，列表显示当前设备的所有端口信息。

图4-3 端口信息

设备信息

端口信息

端口配置

PoE总功率: 5% 5.40W/96.00W

PoE七天峰值功率: 7% 7.60W/96.00W

设备端口列表

编辑

端口号 ▲	别名	PoE功率	PoE状态	PD保活	端口远距离传
1	Ethernet 1/1	0.00W	关闭	关闭	关闭
2	Ethernet 1/2	0.00W	打开	关闭	关闭
3	Ethernet 1/3	0.00W	打开	关闭	关闭
4	Ethernet 1/4	5.40W	打开	关闭	关闭
5	Ethernet 1/5	0.00W	打开	关闭	关闭
6	Ethernet 1/6	0.00W	打开	关闭	关闭
7	Ethernet 1/7	0.00W	打开	关闭	关闭
8	Ethernet 1/8	0.00W	打开	关闭	关闭
9	GigabitEther...	--	未知	未知	未知
10	GigabitEther...	--	未知	未知	未知

步骤3 单击“编辑”，配置端口信息。


表4-2 端口PoE信息

参数	说明
PoE状态	对于支持PoE功能的设备，打开或关闭PoE功能，默认打开。打开或关闭PoE，不影响端口的数据传输。
PD保活	打开PD保活，防止终端设备假死。默认关闭。
端口远距离传输	对于支持远距离功能的设备，开启或关闭远距离开关，默认关闭。 开启远距离功能时，传输距离最远可达到250 m。 启用远距离功能后，端口速率会自动匹配成10 Mbps；禁用后，恢复成自协商。

步骤4 单击“保存”。

4.4 三方设备管理

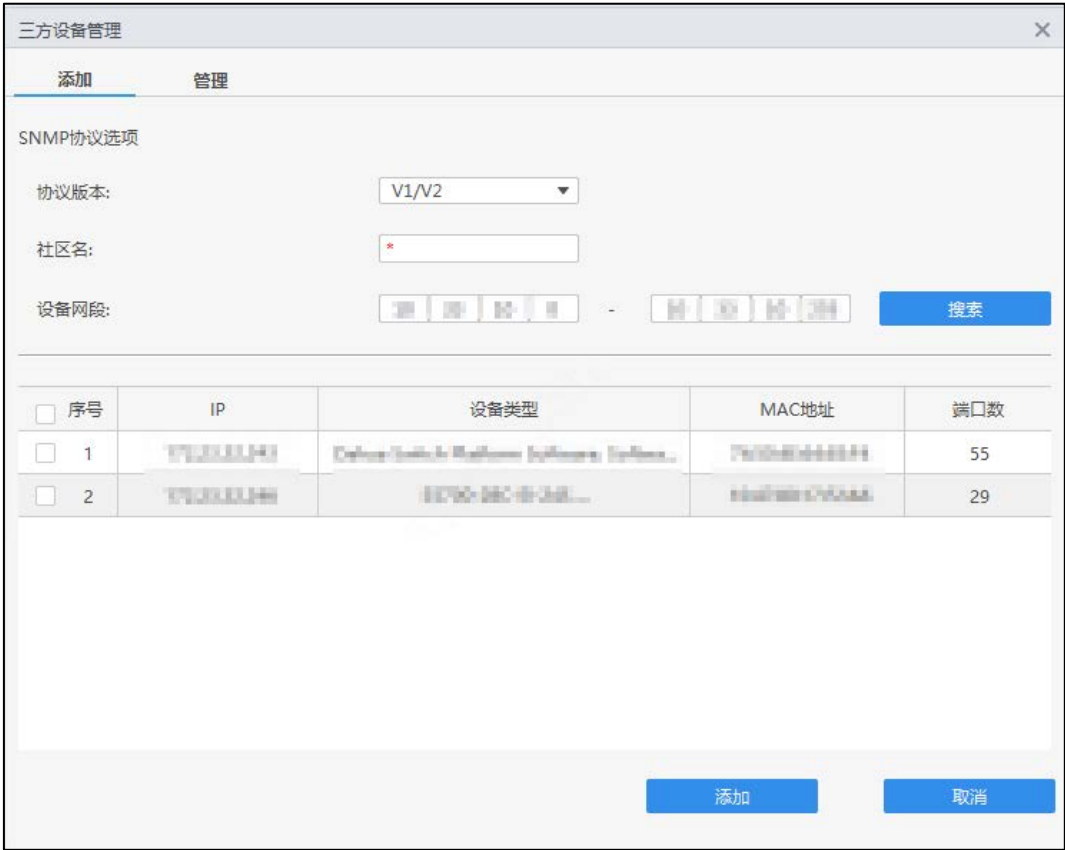
支持第三方管理型（snmp协议管理）交换机发现等功能。

步骤1 在“网络运维”界面单击，管理三方设备。

步骤2 配置三方设备参数。

- 若添加的三方设备是SNMP的V1或者V2版本：

图4-4 添加V1/V2设备



三方设备管理

添加 管理

SNMP协议选项

协议版本: V1/V2

社区名: *

设备网段: 192.168.1.1 - 192.168.1.254 搜索

<input type="checkbox"/> 序号	IP	设备类型	MAC地址	端口数
<input type="checkbox"/> 1	192.168.1.1	Delia Switch Platform Software System...	780040000000	55
<input type="checkbox"/> 2	192.168.1.2	192.168.1.2...	192.168.1.2...	29

添加 取消

表4-3 V1/V2设备参数配置

参数	描述
社区名	配置SNMP的V1版本或者V2版本时所需要的community名字。
设备网段	设备所在局域网的IP地址范围。

- 若添加的三方设备是SNMP的V3版本：

图4-5 添加V3设备

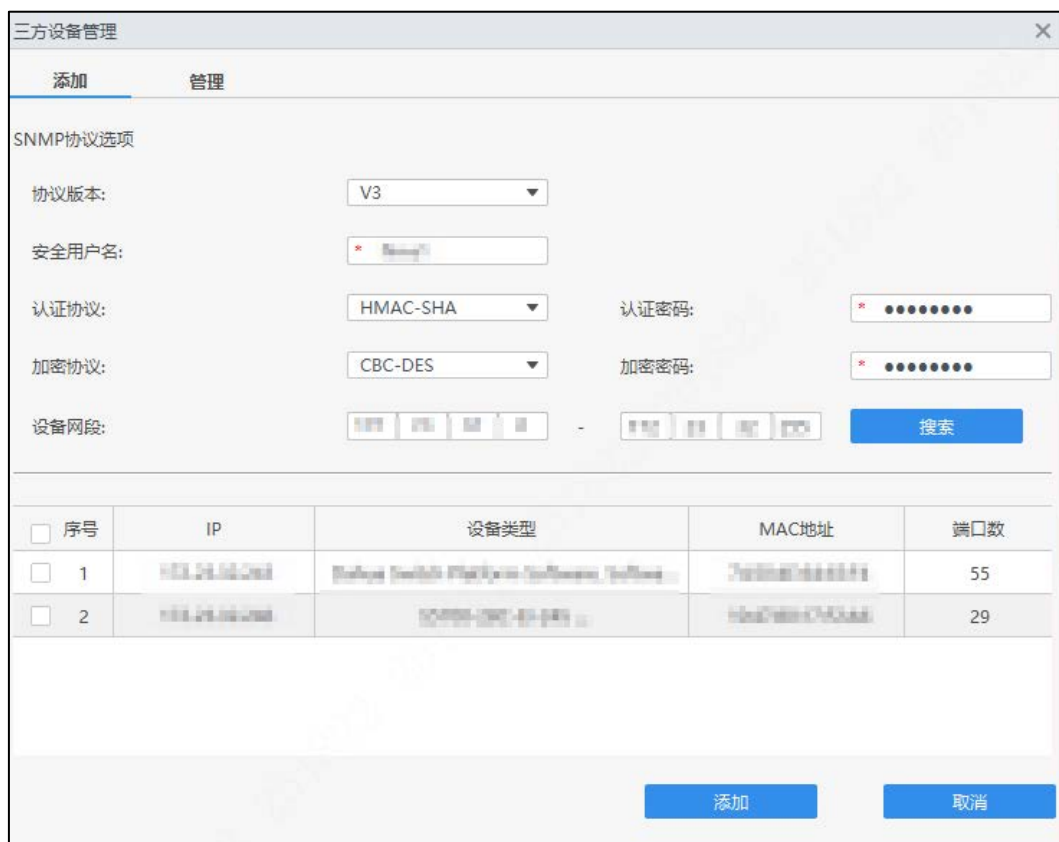


表4-4 V3设备参数配置

参数	描述
安全用户名	配置V3设备的用户名称。
认证协议	SNMP的V3版本中的数据认证协议模式。
认证密码	对应认证协议的密码。
加密协议	SNMP的V3版本连接时的数据加密协议。
加密密码	加密协议设置的密码。
设备网段	设备所在局域网的IP地址范围。

步骤3 配置完成后，单击“搜索”。

步骤4 选择需要添加的设备，单击“添加”。

步骤5 单击“管理”，查看已添加的三方设备。




单击, 删除此项设备信息。

图4-6 查看添加设备

三方设备管理					
添加		管理			
序号	IP	设备信息	Mac地址	在线状态	操作
1	192.168.1.100	Camera Serial: 1234567890123456...	88-88-88-88-88-88	● 在线	
2	192.168.1.101	Camera Serial: 1234567890123456...	88-88-88-88-88-88	● 在线	

4.5 处理报警


当设备状态为异常（红色）时，可选择处理报警。

步骤1 在主界面，右键单击异常设备，选择“处理报警”。

图4-7 处理报警

处理报警					
 批量报警消除					
<input type="checkbox"/>	报警时间	端口号	报警类型	备注	操作
<input type="checkbox"/>	2021-03-27 14:18:01	4	端口掉电		
<input type="checkbox"/>	2021-03-27 14:17:41	4	端口掉电		
<input type="checkbox"/>	2021-03-27 04:50:10	4	端口掉电		
<input type="checkbox"/>	2021-03-27 04:50:10	3	端口掉电		
<input type="checkbox"/>	2021-03-27 02:27:01	4	端口掉电		
<input type="checkbox"/>	2021-03-27 02:26:37	4	端口掉电		

步骤2 消除报警。

- 消除单条报警：单击操作列的.
- 批量消除报警：选择多条报警记录，单击“批量报警消除”，单击“确定”。

第 5 章 查询运维记录

操作步骤

- 步骤1 打开运维中心方案，选择“运维记录”。
- 步骤2 输入查询参数，单击“搜索”。
- 在右侧列表中可查看运维记录的详细信息。

图5-1 运维记录

事件发生时间	设备名称	设备IP	端口	MAC地址	报警类型	备注	处理状态
2021-03-24 1...	--	...	环路报警	2	已处理
2021-03-24 1...	--	...	IP冲突	冲突设备...	已处理
2021-03-24 1...	6	...	端口拨密		已处理
2021-03-24 1...	1	...	端口插电		已处理
2021-03-24 1...	2	...	端口插电		已处理
2021-03-24 1...	3	...	端口插电		已处理
2021-03-24 1...	4	...	端口插电		已处理
2021-03-24 1...	1	...	端口上电		已处理
2021-03-24 1...	3	...	端口上电		已处理
2021-03-24 1...	4	...	端口上电		已处理
2021-03-24 1...	--	...	环路报警	2	已处理
2021-03-24 1...	--	...	IP冲突	冲突设备...	已处理
2021-03-24 1...	2	...	端口上电		已处理
2021-03-24 1...	--	...	环路报警	2	已处理
2021-03-24 1...	--	...	IP冲突	冲突设备...	已处理
2021-03-24 1...	4	...	端口拨密		已处理
2021-03-24 1...	--	...	环路报警	2	已处理
2021-03-24 1...	--	...	IP冲突	冲突设备...	已处理
2021-03-24 1...	--	...	环路报警	2	已处理
2021-03-24 1...	--	...	IP冲突	冲突设备...	已处理

相关操作

导出记录：选择记录，单击“导出”，导出选中记录列表至本地。

附录1 法律声明

版权声明

© 2021 浙江大华技术股份有限公司。版权所有。

在未经浙江大华技术股份有限公司（下称“大华”）事先书面许可的情况下，任何人不能以任何形式复制、传递、分发或存储本文档中的任何内容。

本文档描述的产品中，可能包含大华及可能存在的第三人享有版权的软件。除非获得相关权利人的许可，否则，任何人不能以任何形式对前述软件进行复制、分发、修改、摘录、反编译、反汇编、解密、反向工程、出租、转让、分许可等侵犯软件版权的行为。

商标声明

- 、、、、**HDCVI**是浙江大华技术股份有限公司的商标或注册商标。
- HDMI标识、HDMI和High-Definition Multimedia Interface是HDMI Licensing LLC的商标或注册商标。本产品已经获得HDMI Licensing LLC授权使用HDMI技术。
- 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。

出口管制合规声明

大华遵守适用的出口管制法律法规，并且贯彻执行与硬件、软件、技术的出口、再出口及转让相关的要求。就本手册所描述的产品，请您全面理解并严格遵守国内外适用的出口管制法律法规。

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档中任何信息的权利，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

安全声明

- 若您将产品接入互联网需自担风险，包括但不限于可能遭受网络攻击、黑客攻击、病毒感染等，请您加强网络、设备数据和个人信息等的保护，采取保障设备网络安全的必要措施，包括但不限于修改出厂默认密码并使用强密码、定期修改密码、将固件更新至最新版本等。本公司不对因此造成的产品工作异常、信息泄露等问题承担任何责任，但本公司会提供产品相关安全维护。
- 在适用法律未明令禁止的程度下，对于因使用或无法使用本产品或服务而引起的任何利润、收入、销售损失、数据丢失或采购替代商品或服务的成本、财产损害、人身伤害、业务中断、商业信息损失，或者任何特殊的、直接的、间接的、附带的、经济性、覆盖性、惩罚性、特殊或从属损害，无论是基于何种责任理论（合同、侵权、过失或其他），本公司及其员工、许可方或附属公司都不承担赔偿责任，即使其已被告知存在此种损害的可能性也是如此。某些司法管辖区不允许对人身伤害、附带或从属损害等进行责任限制，则此限制可能不适用于您。
- 本公司对您的所有损害承担的总责任限额（除了因本公司过失导致人身伤亡的情况，需遵循适用法律规定）不超过您购买本公司产品所支付的价款。

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

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。

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。

更多内容

请访问大华官网安全应急响应中心，获取安全公告和最新的安全建议。

「 让社会更安全 让生活更智能 」
ENABLING A SAFER SOCIETY AND SMARTER LIVING