



SmartPSS Plus 访客方案











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
V1.0.3	更新界面图。	2021.03
V1.0.2	新增人事管理。	2020.12
V1.0.1	新增访客自动登记功能说明。	2020.09
V1.0.0	首次发布。	2020.06

目录




前言	I
第 1 章 简介	1
第 2 章 打开访客方案	2
第 3 章 访客登记	3
3.1 手动登记	3
3.2 自动登记	4
第 4 章 人事管理	8
4.1 人事管理	8
4.1.1 创建组织	8
4.1.2 （可选）设置发卡器类型	10
4.1.3 添加人员	10
4.1.4 设置人员权限认证方式	13
4.1.5 配置人员权限	16
4.2 权限配置	17
4.2.1 新增权限组	17
4.2.2 关联人员	18
4.3 授权进度	19
4.4 自动采集	19
4.4.1 实时采集	19
4.4.2 提取采集记录	20
第 5 章 查看访客记录	22
附录 1 法律声明	23
附录 2 网络安全声明和建议	25


第 1 章 简介

传统访客登记的步骤是前台、保安或访客自己手动填写个人信息，耗时而且不能确定访客的真实身份。SmartPSS Plus 访客方案将带有身份证读取功能的智能身份核验终端和 SmartPSS Plus 配合使用，访客将身份证放在智能身份核验终端的身份证读取区域，智能身份核验终端自动将访客身份信息上传到 SmartPSS Plus，再通过 SmartPSS Plus 授予访客门禁设备刷卡和刷脸通行权限。使用本方案，无需手动登记访客信息，访客自行在具有权限的门禁设备刷卡或刷脸通行，节省时间也能保证访客身份，同时访客信息被储存在 SmartPSS Plus 访客数据库里，用户能方便快速地查找访客身份，不用一页页翻查纸质的访客登记本，大幅提升工作效率。

第 2 章 打开访客方案

不同场景打开访客方案的操作方法不同。

- 如果是首次使用 SmartPSS Plus，登录过程中加载访客方案。登录后，在主页的左侧导航栏单击 ，打开访客方案。
- 如果已打开 SmartPSS Plus，但未加载访客方案，在界面右上角选择“ > 切换方案”，加载访客方案。登录后，在主页的左侧导航栏单击 ，打开访客方案。

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

第3章 访客登记


访客登记是指在 SmartPSS Plus 录入访客信息，并授予访客门禁刷卡和刷脸通行权限。

按照授权方式不同，访客登记方式有两种，请按需选择。

- 方式一：手动登记。访客在智能身份核验终端上刷身份证后，系统自动获取访客信息，选择补充详细信息后，手动授予访客门禁设备刷卡和刷脸通行权限。
- 方式二：自动登记。预先配置人脸门禁一体机自动授予刷脸通行权限。配置后，人员在智能身份核验终端刷身份证后，系统自动授予该访客人脸门禁一体机的刷脸通行权限，而无需手动授予。

3.1 手动登记

前提条件

选择“主页 > 设备管理”，添加智能身份核验终端到系统，详细介绍请参见 SmartPSS Plus 使用说明书。在界面右上角选择“ > 帮助手册”，获取 SmartPSS Plus 使用说明书。

操作步骤

步骤1 打开访客方案，在主页单击“访客登记”页签。

步骤2 根据实际情况进入到访客登记界面。

- 如果访客携带身份证，访客在智能身份核验终端上刷身份证，进入访客登记界面。
- 如果访客未携带身份证，单击“添加”，进入访客登记界面。

图3-1 访客登记

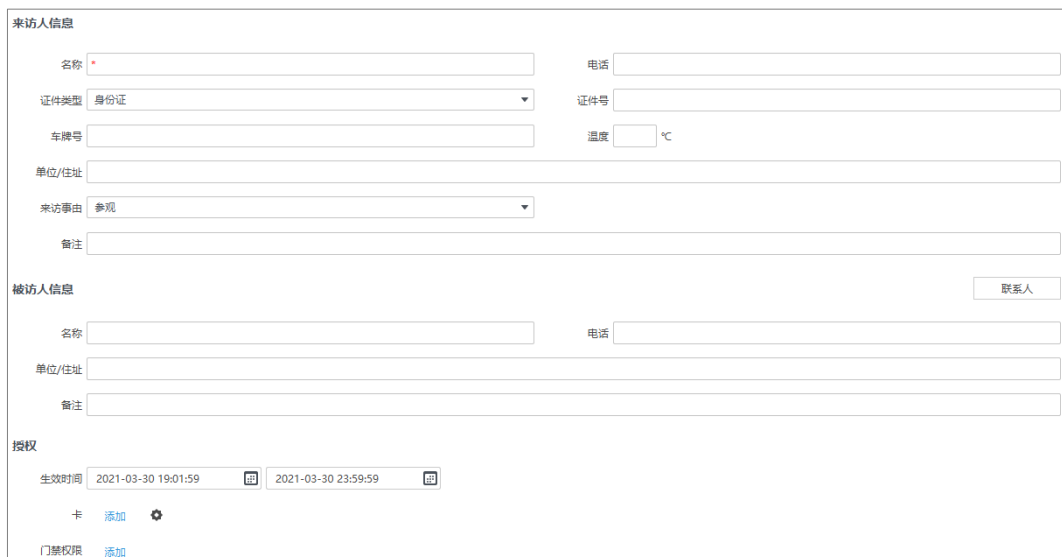



图3-1展示了访客登记的操作界面，分为三个主要部分：

- 来访人信息**：包含名称、电话、证件类型（身份证）、证件号、车牌号、温度（℃）、单位/住址、来访事由（参观）、备注等输入项。
- 被访人信息**：包含名称、电话、单位/住址、备注等输入项，右侧有“联系人”按钮。
- 授权**：包含生效时间（2021-03-30 19:01:59 至 2021-03-30 23:59:59）、卡（添加）、门禁权限（添加）等选项。

步骤3 采集访客人脸。采集后，访客在具有权限的门禁可以刷脸开门。

访客面对智能身份核验终端摄像头，确保访客人脸在采集画面绿框区域，单击采集画面

右上角的.

步骤4 填写来访人信息。

步骤5 填写被访人信息或单击“联系人”在弹出的对话框选择被访人。


说明

需要先添加被访人到系统，才能通过“联系人”添加被访人。通过“主页 > 人事管理”添加被访人到系统，详细介绍请参见 SmartPSS Plus 考勤或门禁方案使用说明书。

步骤6 在“授权”区域设置访客具有的门禁权限有效时间。

超出该时间后，权限失效，同时访客状态自动切换为离访状态。

步骤7 授予访客刷卡通行权限。

- 方式一：手动授予。在“卡”区域单击“添加”，在弹出的对话框手动输入访客卡号，单击“确定”。
- 方式二：通过读卡设备授予。在“卡”区域单击右侧的，在弹出的对话框选择读卡设备，单击“确定”；然后单击“添加”，在读卡设备上刷卡，系统自动读取卡号，单击“确定”。

说明

如果通过读卡设备授予刷卡权限，请确保已连接读卡设备，读卡设备例如发卡器或具有刷卡功能的门禁设备。

步骤8 授予访客门禁设备权限。在“门禁权限”区域单击“添加”，在弹出的界面选择访客可以刷卡/刷脸开门的门禁设备，单击“确定”。


步骤9 单击“保存”。

相关操作

编辑访客信息。在访客登记界面右侧单击要编辑信息的访客，在左侧界面编辑访客信息，单击“保存”。

3.2 自动登记

前提条件

- 选择“主页 > 设备管理”，添加智能身份核验终端和人脸门禁一体机到系统，详细介绍请参见 SmartPSS Plus 使用说明书。在界面右上角选择“ > 帮助手册”，获取 SmartPSS Plus 使用说明书。
- 仅人脸门禁一体机支持配置自动授权。

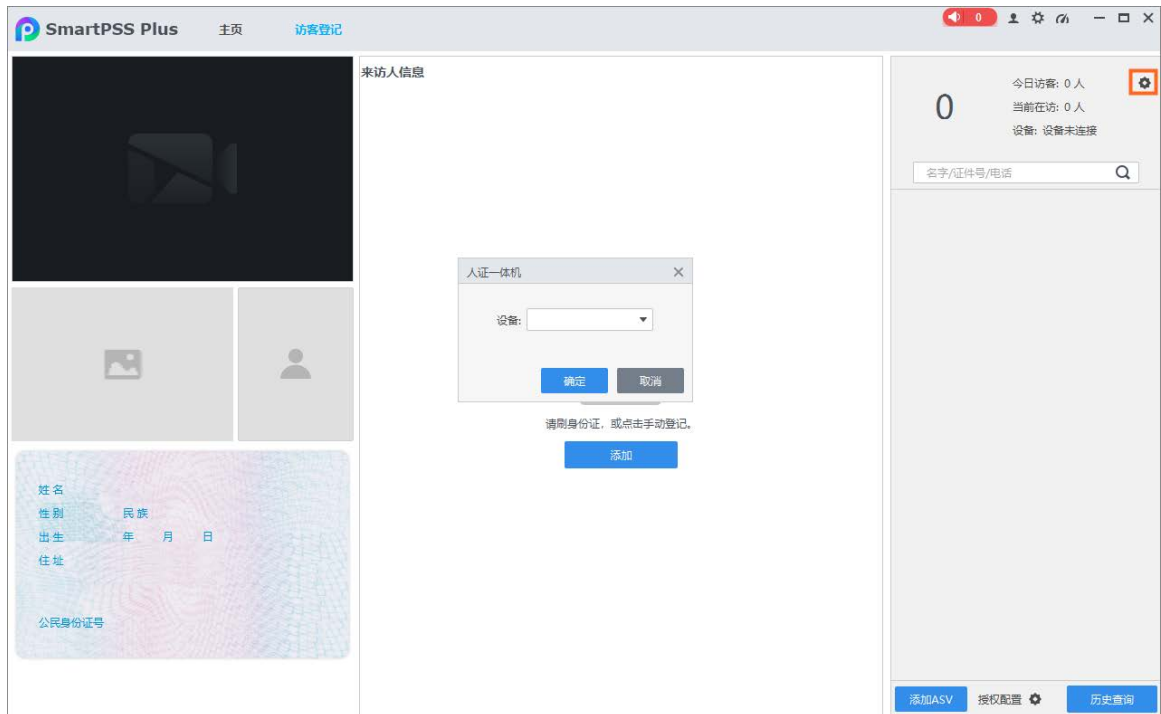
操作步骤

步骤1 打开访客方案，在主页单击“访客登记”。
进入访客登记界面。

步骤2 选择登记设备。

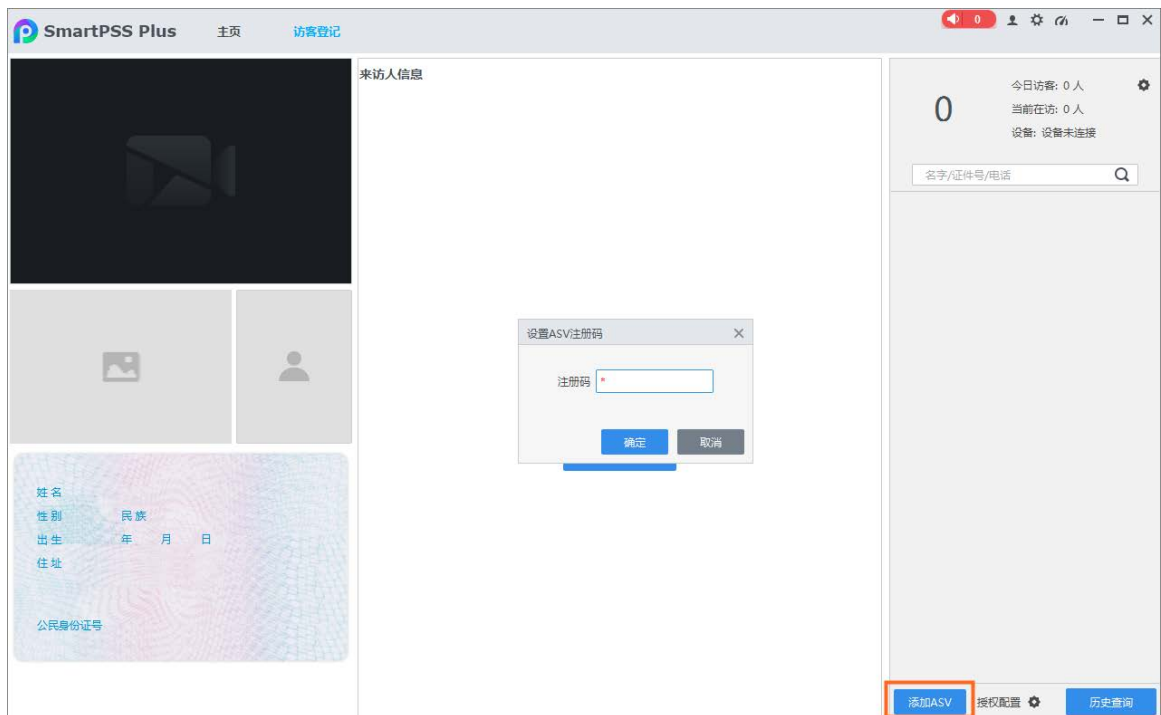
- 单击界面右上角 ，选择人证一体机设备，单击“确定”。

图3-2 选择人证一体机



- 单击界面右下方“添加 ASV”，输入第三方访客机设备的注册码，单击“确定”。

图3-3 添加 ASV

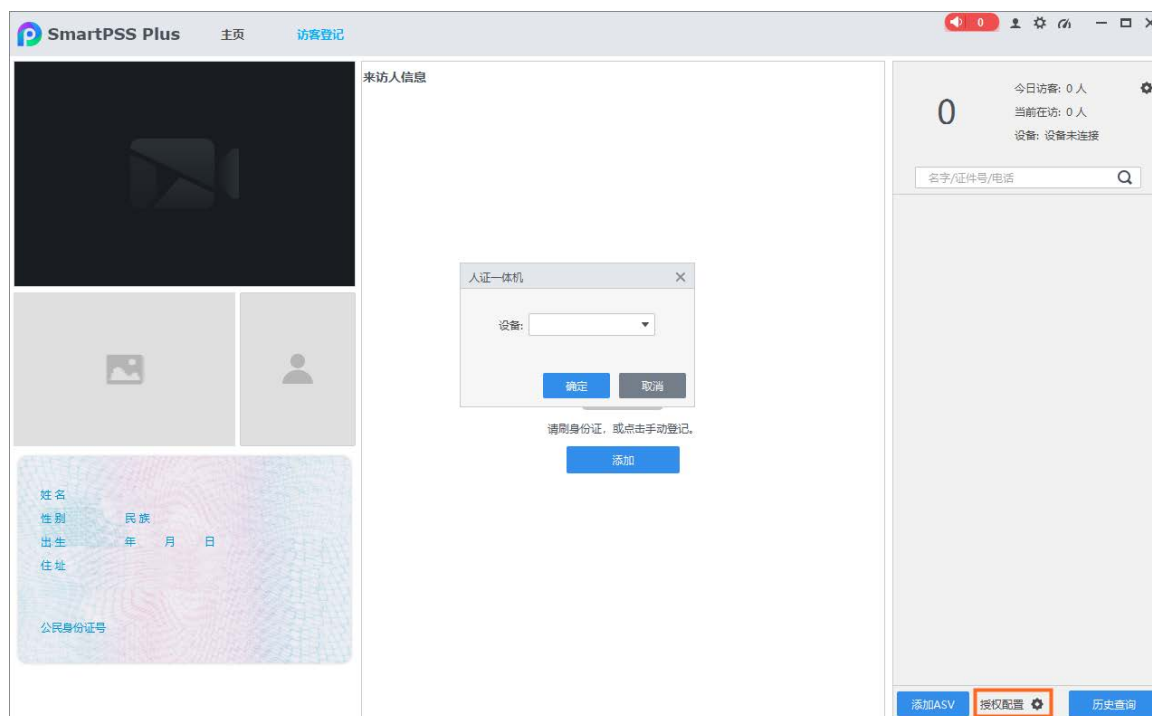


说明

当平台连接第三方访客机设备时，不展示访客采集画面，仅上传设备抓拍的照片。

步骤3 在“访客登记”界面右下角单击“授权配置”。

图3-4 授权配置（1）



步骤4 在弹出的对话框配置自动授权。

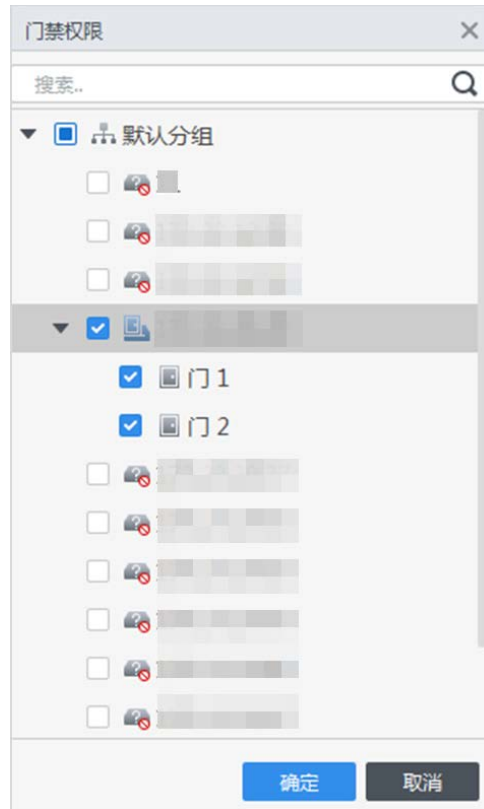
1. 开启“自动授权”功能。
2. 在“授权期限”栏设置授权期限。
3. 单击“选择门”右侧的 ⚙️，在弹出的对话框选择需要自动授权的人脸门禁一体机，单击“确定”。

授权期限内访客在该人脸门禁一体机具有刷脸通行权限。

图3-5 授权配置（2）



图3-6 授权配置 (3)



- 步骤5** 访客在智能身份核验终端上刷身份证。
系统自动将访客人脸下发到已配置自动授权的人脸门禁一体机，该人员在已配置自动授权的人脸门禁一体机可直接刷脸通行。
- 步骤6** （可选）如果需要赋授予访客刷卡通行权限，在“访客登记”界面右侧单击需要授予刷卡通行权限的访客卡片，在左侧界面通过如下任意一种方式授予访客刷卡权限。
- 方式一：手动授予。在“卡”区域单击“添加”，在弹出的对话框手动输入访客卡号，单击“确定”。
 - 方式二：通过读卡设备授予。在“卡”区域单击右侧的⚙️，在弹出的对话框选择读卡设备，单击“确定”；然后单击“添加”，在读卡设备上刷卡，系统自动读取卡号，单击“确定”。

说明

如果通过读卡设备授予刷卡权限，请确保已连接读卡设备，读卡设备例如发卡器或具有刷卡功能的门禁设备。

- 步骤7** 单击“保存”。

第4章 人事管理

人事管理包含在 SmartPSS Plus 中创建组织人员架构、配置组织中的人员权限、查看授权的进度与状态、自动采集设备中的人员信息等功能。

4.1 人事管理

用于创建组织架构，录入组织人员，配置人员权限等。

4.1.1 创建组织

用于创建公司、添加各级部门。

步骤1 打开访客方案，在主页单击“人事管理”。

步骤2 在左侧导航栏单击.

步骤3 输入公司信息。


1. 在部门组织树选择公司名称，单击.

图4-1 编辑公司信息



2. 在“公司信息”界面填写公司信息，单击“确定”。

图4-2 填写公司信息



公司信息

公司: * 公司A

传真: 11406789

电子邮件: 11406789@11406789.com

电话: 11406789

网址: 11406789.com

邮政编号: 114067

地址1: 11406789 114

地址2: 114067 114

LOGO

图片大小: 建议小于100KB

步骤4 创建部门。

1. 在部门组织树单击 **+**。

图4-3 创建部门 (1)



部门组织树

+ -

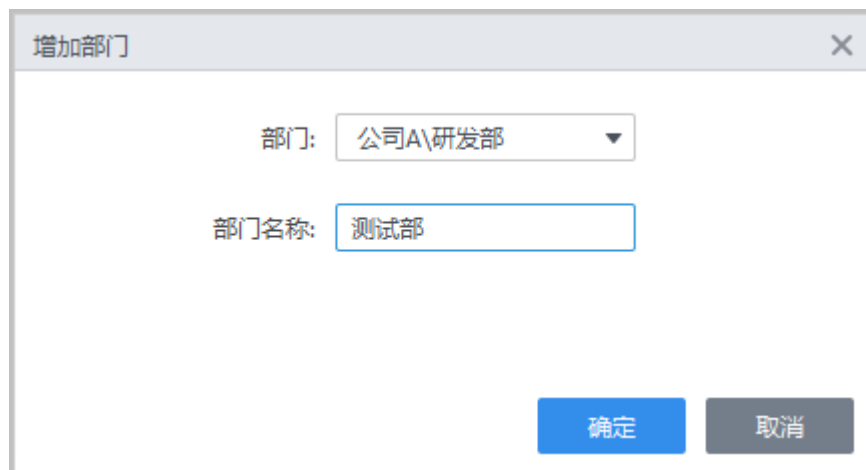
搜索..

公司A(3)

研发部(1)

2. 在弹出的对话框中选择上级部门，输入部门名称，单击“确定”。

图4-4 创建部门 (2)





增加部门

部门: 公司A\研发部

部门名称: 测试部

确定 取消


相关操作

- 修改部门名称：在导航树选择待修改的部门，单击，修改部门名称。
- 删除部门：在导航树选择待删除的部门，单击.

4.1.2 （可选）设置发卡器类型

通过发卡器读取人员卡号时，需确保设置的发卡类型与实际使用的发卡器类型一致，否则可能无法自动读取卡号。系统默认发卡器类型为 IC 卡。

步骤1 打开访客方案，在主页单击“人事管理”。

步骤2 在左侧导航栏单击，单击“发卡类型”。

步骤3 选择实际使用的发卡器类型，单击“确定”。

图4-5 设置系统端发卡器类型




4.1.3 添加人员

通过以下任意一种方式向系统中添加人员：

- 单个添加人员。
- 批量添加人员。
- 从带有人员信息的设备中提取人员信息。
- 从本地导入人员信息到系统。

4.1.3.1 单个添加人员

步骤1 打开访客方案，在主页单击“人事管理”。

步骤2 在左侧导航栏单击，单击“添加”。

步骤3 单击“基本信息”，输入人员基本信息。


步骤4 （可选）单击人员照片上的操作，根据提示上传人员照片。

- 身份证读取：在人证设备上刷身份证，录入身份证上的人员照片。
- 摄像抓图：抓取设备拍摄的人员头像，上传到人员照片。
- 上传图片：从本地上传一张图片，作为该人员照片。

说明

- 每个人最多可上传两张照片。
- 使用人证设备摄像抓图时，请将设备设置为“协同采集模式”。

图4-6 输入人员基本信息



步骤5 （可选）设置人员权限认证方式及配置人员权限。

详细介绍请参见 4.1.4 设置人员权限认证方式和 4.1.5 配置人员权限。

步骤6 单击“完成”。

4.1.3.2 批量添加人员

步骤1 打开访客方案，在主页单击“人事管理”。

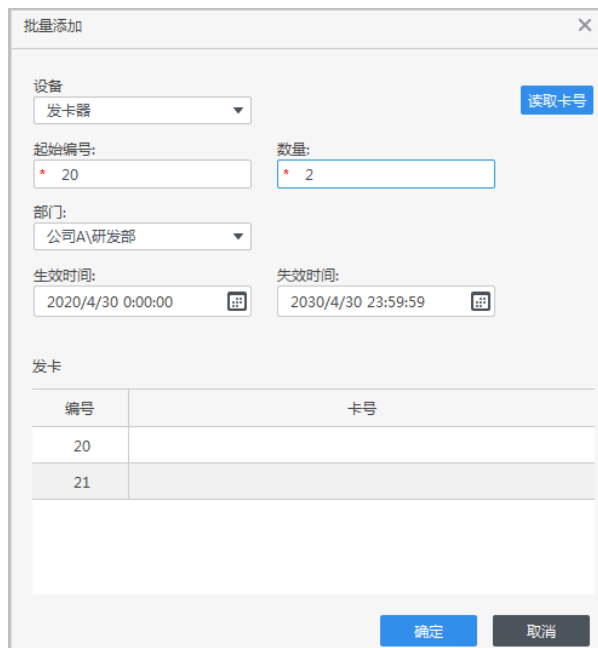
步骤2 在左侧导航栏单击 ，单击“批量添加”。

步骤3 设置人员起始编号和人员数量，选择人员所属部门，设置卡片生效和失效时间。

步骤4 发卡。在“设备”下拉列表框选择读卡设备，单击“读取卡号”。在读卡设备上刷卡后，系统会自动读取人员卡号到列表。

步骤5 单击“确定”。

图4-7 批量添加人员



批量添加

设备: 发卡器 读取卡号

起始编号: * 20 数量: * 2

部门: 公司A\研发部

生效时间: 2020/4/30 0:00:00 失效时间: 2030/4/30 23:59:59

发卡

编号	卡号
20	
21	

确定 取消

4.1.3.3 从设备中提取人员信息


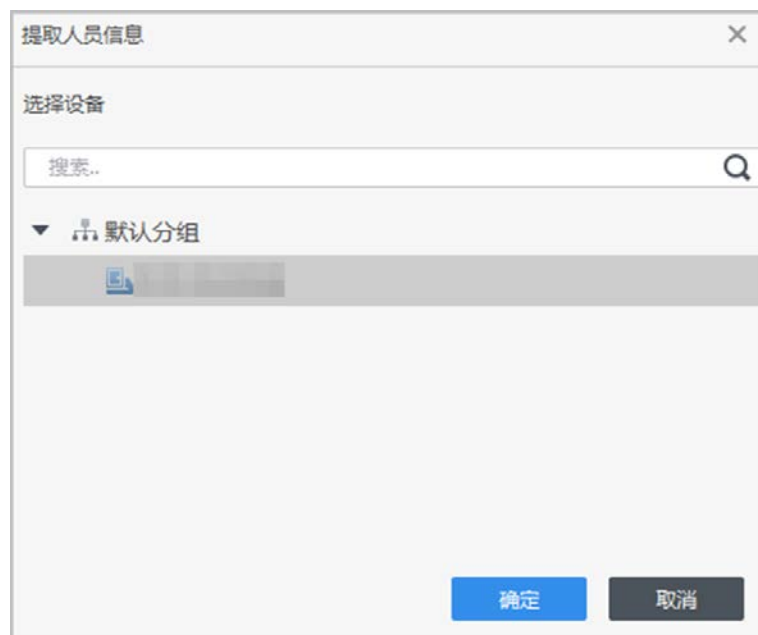
- 步骤1 打开访客方案，在主页单击“人事管理”页签。
- 步骤2 在左侧导航栏单击 ，单击“提取”。
- 步骤3 在设备树中，选择要提取人员信息的设备，单击“确定”。

图4-8 选择带有人员信息的设备




提取人员信息

选择设备

搜索.. Q

默认分组



确定 取消

- 步骤4 选择需要提取的人员信息，单击“提取”。

图4-9 提取人员信息

提取人员信息

设备名称:

编号/姓名/卡号

Q


<input checked="" type="checkbox"/>	序号	编号 ▼	名称	卡号	人员类型	部门	指纹数
<input checked="" type="checkbox"/>	1	888	888	159F82E9	普通用户		0

提取

导出



取消

4.1.3.4 从本地导入人员

- 步骤1 打开访客方案，在主页单击“人事管理”页签。
- 步骤2 在左侧导航栏单击  页签，单击“导出”，导出人员信息模板到本地，按照模板填写人员信息。
- 步骤3 单击“导入”，在弹出的对话框中选择人员信息表，根据提示导入人员。

4.1.4 设置人员权限认证方式

操作步骤

- 步骤1 打开访客方案，在主页单击“人事管理”。
- 步骤2 在左侧导航栏单击 .
- 步骤3 在人员列表单击 ，单击“认证”页签。
- 步骤4 设置认证方式。
- 设置人员密码。
在“密码”区域，单击“添加”，输入密码。



说明

部分设备密码最多支持 6 位。如果使用设置的密码无法打开设备，请尝试将密码修改到 6 位或 6 位以内，再使用该密码开锁。

图4-10 设置人员密码



添加用户

基本信息 认证 权限配置

密码 添加 ⚠ 针对二代门禁设备是人员密码，否则是卡密码。

新密码: *

密码确认: *

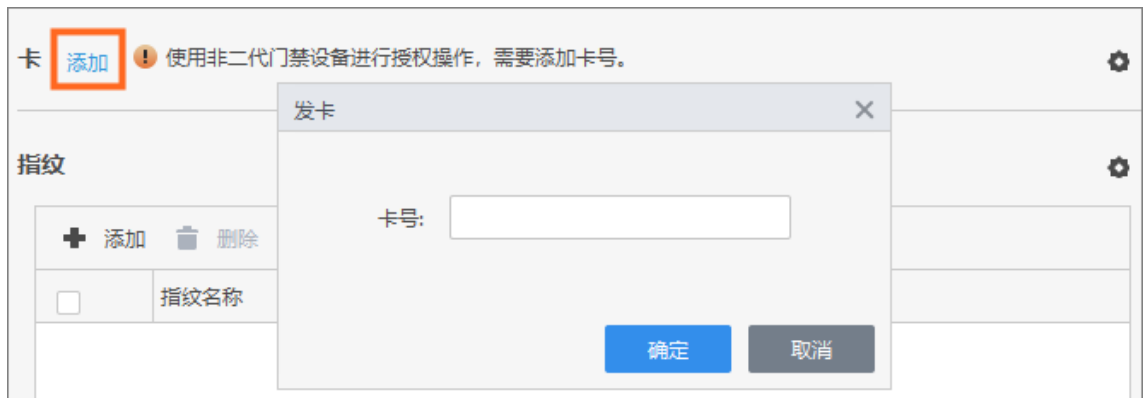
确定 取消

- 绑定人员卡号。
绑定后，人员可以使用该卡验证设备权限。

说明

- 最多支持添加 5 张卡，支持设置 1 张胁迫卡、设置 1 张主卡。
- 通过读卡设备读取卡号时，需确保系统端设置的读卡器类型与实际读卡设备类型一致，详细介绍请参见“4.1.2（可选）设置发卡器类型”。
 - ◇ 方式一：单击“添加”，在弹出的对话框手动输入人员卡号，单击“确定”。

图4-11 绑定人员卡号方式一



卡 添加 ⚠ 使用非二代门禁设备进行授权操作，需要添加卡号。

指纹

+ 添加 - 删除

指纹名称

发卡

卡号:

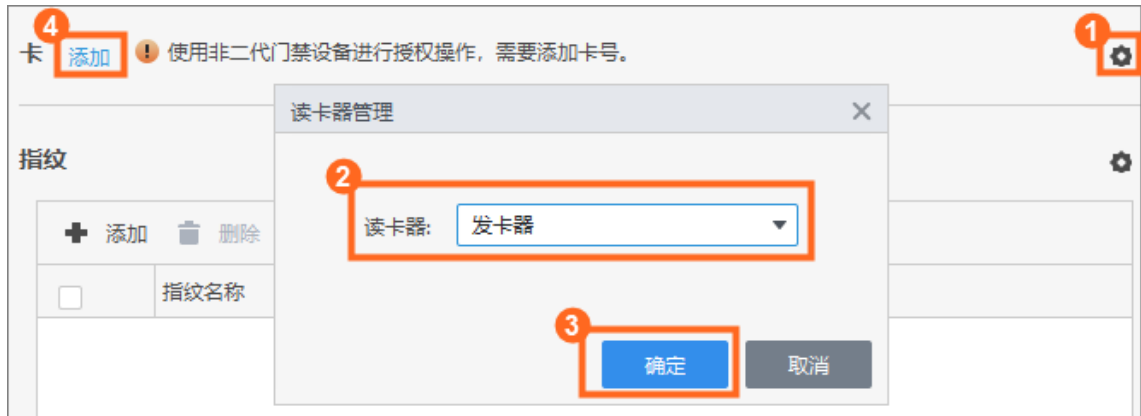
确定 取消

- ◇ 方式二：单击右侧的 ⚙，在弹出的对话框选择读卡设备，单击“确定”；然后单击“添加”，在读卡设备上刷卡，系统自动读取卡号，单击“确定”。

说明

使用人证设备发卡时，请将设备设置为“协同采集模式”。

图4-12 绑定人员卡号方式二



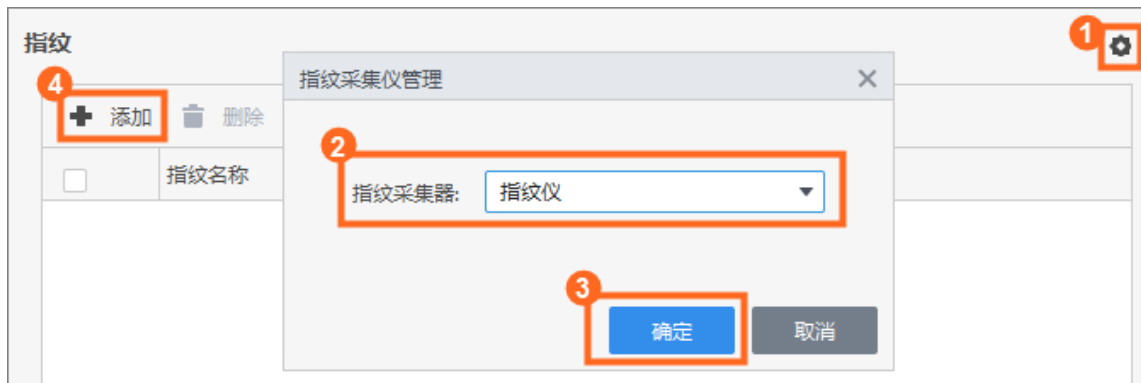
- 录入人员指纹。

在“指纹”区域单击右侧的⚙️，在弹出的对话框选择指纹采集设备，然后在“指纹”区域单击“添加”，根据提示在设备上录入指纹。

说明

- 最多支持上传 3 个指纹，支持设置 1 个胁迫指纹。
- 使用人证设备采集指纹时，请将设备设置为“协同采集模式”。

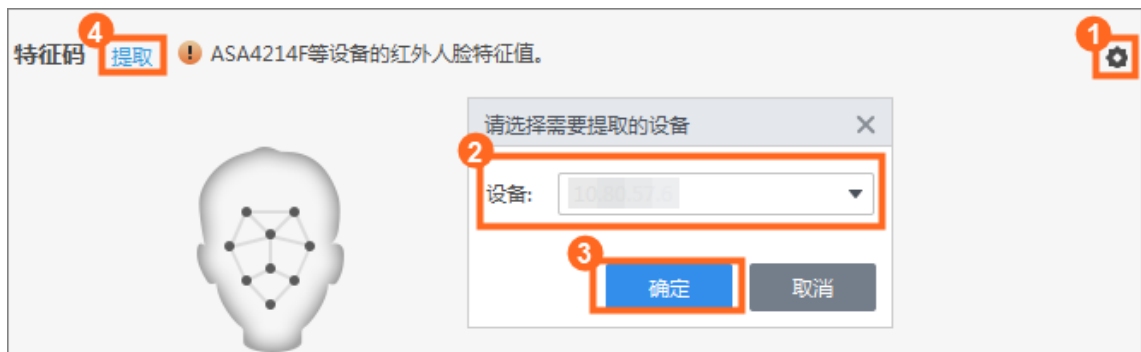
图4-13 录入人员指纹



- 上传人员特征码。

在“特征码”区域单击⚙️。选择已上传该人员人脸特征值的设备，单击“确定”。单击“提取”。

图4-14 配置特征码



步骤5 单击“完成”。

相关操作


批量发卡。

用于批量给已添加但未发卡的多个人员发卡。

说明

通过读卡设备读取卡号时，需确保系统端设置的读卡器类型与实际读卡设备类型一致，详细介绍请参见“4.1.2（可选）设置发卡器类型”。

步骤1 打开访客方案，在主页单击“人事管理”页签。

步骤2 在左侧导航栏单击页签，在人员列表选择需要发卡的人员，单击“批量发卡”。

步骤3 批量发卡。卡号支持通过刷卡自动读取或手动填写。

- 通过刷卡自动读取卡号。在“设备”栏选择使用的读卡设备，单击“读取卡号”，然后按照人员列表中的顺序，依次放置对应人员的卡片，系统自动读取卡号；编辑每位人员的其他信息，例如卡片的有效时间范围等。
- 手动输入卡号。在人员列表依次选择人员，填写人员的卡号等信息。

图4-15 批量发卡



批量发卡

设备: 发卡器 读取卡号

编号: 30 名称:

卡号: 12345 部门: 研发部

开始时间: 2020-04-30 00:00:00 结束时间: 2030-04-30 23:59:59

人员列表

编号	名称	卡号	操作
30		00012345	
31			

确定 取消


步骤4 单击“确定”。

4.1.5 配置人员权限

为人员设置权限，分为绑定用户权限组和绑定设备两种方式。

步骤1 打开访客方案，在主页单击“人事管理”。

步骤2 在左侧导航栏单击 。

步骤3 在人员列表单击 ，单击“权限配置”。

步骤4 配置人员权限。

- 用户组：绑定用户权限组，从而使该人员具有权限组中的权限。
选择“用户组”，在列表中选择需要绑定的权限组。配置权限组的详细介绍请参见 4.2.1 新增权限组。
- 设备：将该用户与设备绑定，从而使该人员具有该设备的权限。
选择“设备”，选择权限类型为“门禁权限组”，选择需要绑定的设备并选择时间模板。

步骤5 单击“完成”。


4.2 权限配置

用于管理权限组，将权限组与对应的人员关联起来，从而为人员赋予对应权限组的权限。

4.2.1 新增权限组

将一个或多个设备设置为一个门禁权限组。

步骤1 打开访客方案，在主页单击“人事管理”。

步骤2 在左侧导航栏单击 。


步骤3 单击 ，在弹出的对话框中输入权限组名称，选择权限组类型和时间模板，选择权限认证方式，在设备导航树中选择设备，单击“确定”。

图4-16 添加权限组

增加权限组

基本信息

组名:

权限组2

备注:

权限组类型:

门禁权限组

时间模板:

全时间时间模板

认证方式:

☒ 卡

☒ 指纹

☒ 密码

☒ 人脸

所有设备

已选择 (0)

搜索..

默认分组

4.2.2 关联人员

将配置好的权限组与对应的人员关联起来，从而使这些人员拥有该权限组中的权限。

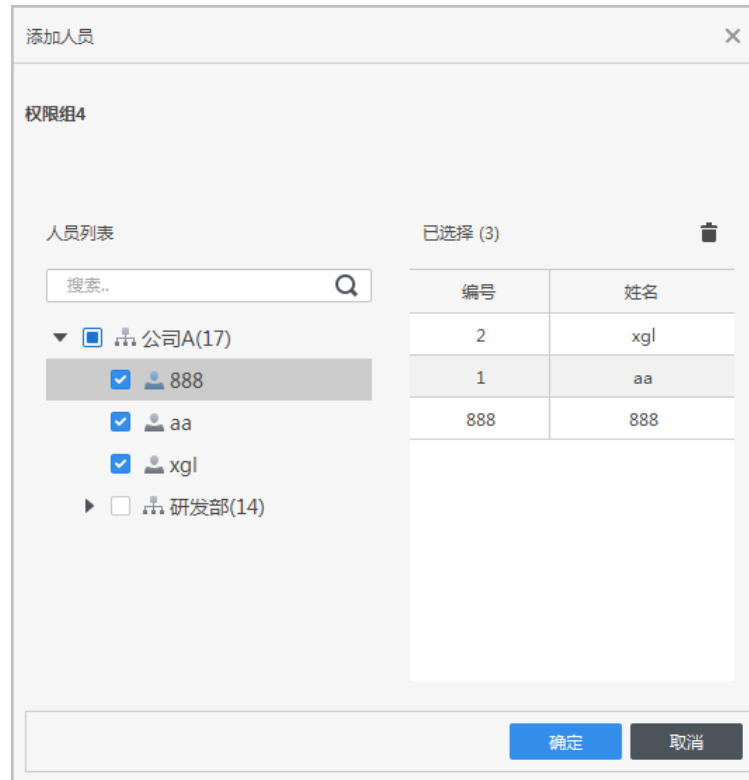
步骤1 打开访客方案，在主页单击“人事管理”。

步骤2 在左侧导航栏单击。

步骤3 单击权限组右侧的。



步骤4 在弹出的界面选择人员，单击“确定”。

图4-17 在权限组中关联人员



4.3 授权进度

查看已配置的人员权限信息下发到设备的进度与结果。

在左侧导航栏单击 ，在右侧界面查看权限下发的进度与结果。如果授权异常，单击操作列的 ，查看异常原因。

4.4 自动采集

将人证核验设备采集的人员信息（身份证、人脸、指纹、卡等）上传到平台。

4.4.1 实时采集


平台开启设备监听。当设备上采集到人员信息时将自动上传到平台。

前提条件

设备端需要配置在线采集模式。详细信息请参见设备配套的使用说明书。

操作步骤

步骤1 打开访客方案，在主页单击“人事管理”。

步骤2 在左侧导航栏单击 。

步骤3 打开“自动采集”。

步骤4 在设备树中选择设备。
此时在设备上采集到的人员信息会出现在右侧采集记录列表中。

说明

- 当采集到重复人员信息时，采集记录列表会覆盖重复信息，只显示最新记录。
- 当采集到已审核的人员信息时，系统提示人员重复。
- 当采集到重复卡号时，系统提示卡号重复。



图4-18 选择自动采集设备




步骤5 （可选）打开“自动审核”。设备采集的人员数据直接变为“审核通过”，同时自动同步到人员数据库中。

若未打开“自动审核”，数据状态为“未审核”，不进入人员数据库，数据需要人工审核后才能真正生效。

步骤6 选择未审核的采集记录，单击上方操作按钮，可执行对应操作。

-  拒绝，该人员信息审核未通过。
-  审核，该人员信息通过，并将此人员添加到人员列表中。


说明


单击  清除，清除列表中已处理的采集记录。数据清理后无法恢复，请谨慎操作。

4.4.2 提取采集记录

将人证核验设备离线采集的人员信息（身份证、人脸、指纹、卡等）批量提取到平台。

步骤1 打开访客方案，在主页单击“人事管理”。

步骤2 在左侧导航栏单击 。

步骤3 在设备树中选择需要提取记录的设备，单击  提取。

步骤4 选择提取日期区间，单击“提取”。

图4-19 提取采集记录



The image shows a 'Manual Extraction' dialog box. It has a title bar with the text '手动提取' and a close button. Inside, there is a label '提取日期:' followed by two date-time pickers. The first picker shows '2020/10/30 0:00:00' and the second shows '2020/11/30 23:59:59', separated by a minus sign. Below this, there is a checked checkbox labeled '重复数据覆盖'. At the bottom right, there are two buttons: '提取' (Extract) and '取消' (Cancel).

说明

- 若选择“重复数据覆盖”，当采集到重复的人员信息时，采集记录列表会覆盖重复信息，只显示最新记录。当采集到重复卡时，解除原有持卡人，当前人作为新的持卡人。
- 若不选择“重复数据覆盖”，当采集到的重复人员信息或卡号时，系统提示人员重复或卡号重复，并只显示最新一条记录。


第 5 章 查看访客记录

操作步骤

- 步骤1 打开访客方案，在主页单击“访客记录”页签或在访客登记界面单击“历史查询”。
- 步骤2 在访客记录界面设置筛选条件，查看访客记录。



说明

- 在访客记录列表双击某访客记录，可查看访客详情。
- 单击访客“操作”列的，查看该访客的开门记录。

相关操作

导出访客记录。在访客记录界面单击“导出”，导出访客记录到本地。

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

- 、、、、 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 网络安全声明和建议

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，包括但不限于使用复杂密码、定期修改密码、及时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、财产损失、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。
- 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。

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