



SmartPSS Plus 门禁方案











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
V1.0.5	修改人事管理权限配置内容。	2021.03
V1.0.4	<ul style="list-style-type: none"> 修改人事管理章节。 新增 6.4 设置门禁点。 	2020.12
V1.0.3	闸机设备新增语音播报和统计进出、清除人数功能。	2020.11
V1.0.2	<ul style="list-style-type: none"> 新增门禁设备记忆和二次开启功能说明。 将事件配置说明移动到 SmartPSS Plus 使用说明书。 更新配置反潜回描述。 	2020.09

版本号	修订内容	发布日期
V1.0.1	<ul style="list-style-type: none">● 更新打开门禁方案、赋予人员门禁权限说明。● 新增首卡开门、多人开门、多门互锁、查看门禁视频、配置远程开门说明。	2020.06
V1.0.0	首次发布。	2020.05

目录



前言	I
第 1 章 简介	1
第 2 章 打开门禁方案	2
第 3 章 门禁向导	3
第 4 章 人事管理	4
4.1 人事管理	4
4.1.1 创建组织	4
4.1.2 （可选）设置发卡器类型	6
4.1.3 添加人员	6
4.1.4 设置人员权限认证方式	9
4.1.5 配置人员权限	12
4.2 权限配置	13
4.2.1 新增权限组	13
4.2.2 关联人员	14
4.3 授权进度	15
4.4 自动采集	15
4.4.1 实时采集	15
4.4.2 提取采集记录	16
第 5 章 门禁配置	18
5.1 创建时间模板	18
5.2 高级配置	20
5.2.1 配置首卡开门	20
5.2.2 配置多人开门	21
5.2.3 配置反潜回	23
5.2.4 配置多门互锁	24
5.3 门禁配置	25
5.4 查询门历史事件	28
第 6 章 门禁管理	29
6.1 远程开关门	29
6.2 设置门常开或常关	30
6.3 查看门禁视频	30
6.3.1 查看单个门禁实时视频	31
6.3.2 查看两个及以上门禁实时视频	31
6.4 设置门禁点	31
6.5 查看门禁详情	32
6.6 重启门禁	33
附录 1 法律声明	34
附录 2 网络安全声明和建议	36

第 1 章 简介

SmartPSS Plus 门禁方案将 SmartPSS Plus 与门禁设备配套使用，提供中小型场景下远程开关门、查看门禁视频、远程设置门禁相关报警等功能。

第 2 章 打开门禁方案

不同场景打开门禁方案的操作方法不同。

- 如果是首次使用 SmartPSS Plus，登录过程中加载门禁方案。登录后，在主页的左侧导航栏单击，打开门禁方案。
- 如果已打开 SmartPSS Plus，但未加载门禁方案，请加载门禁方案，在界面右上角选择“ >”，切换方案”，在加载方案界面加载门禁方案。

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

第 3 章 门禁向导

门禁向导专门为首次使用门禁方案的用户量身打造，提供一套从门禁业务配置到门禁异常处理、门禁数据查询和统计的完整门禁业务流程。通过门禁向导，可以帮助您快速搭建并使用门禁业务。

门禁向导的使用方法如下：


步骤1 打开门禁方案，在主页单击“门禁向导”。

步骤2 按照图 3-1 所示顺序配置门禁业务。

图3-1 配置门禁业务



表3-1 配置和使用门禁业务说明

序号	模块	配置任务
1	设备管理	添加门禁设备，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”获取该文档。
2	人事管理	创建组织、添加人员并赋予人员设备的权限，详细介绍请参见“4.1 人事管理”。
3	时间模板	创建时间模板，详细介绍请参见“5.1 创建时间模板”。
4	权限组	赋予人员门禁通行权限，详细介绍请参见“4.2 权限配置”。
5	门禁管理	使用门禁业务，例如远程开关门、设置门常开或常关、查看门禁视频等，详细介绍请参见“第 6 章门禁管理”。

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 打开门禁方案，在主页单击“人事管理”或在门禁向导单击.

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



步骤4 创建部门。


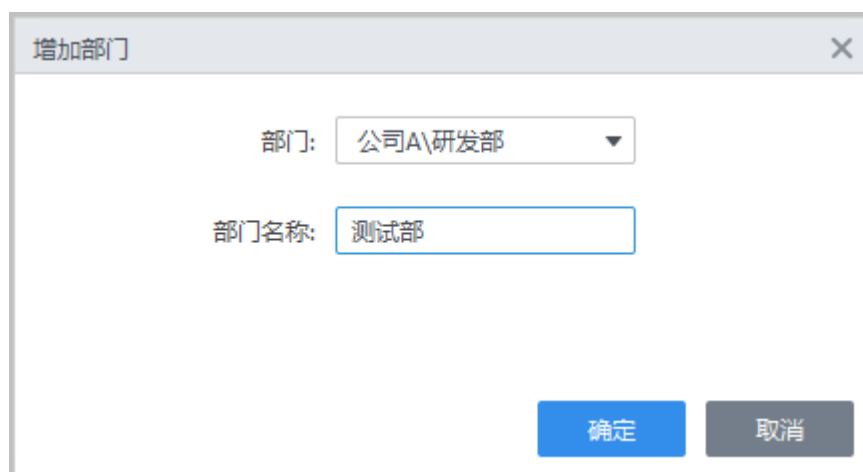
1. 在部门组织树单击 。

图4-3 创建部门 (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)





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

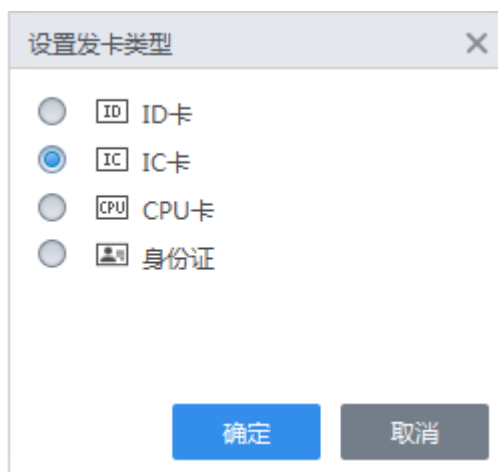
通过发卡器读取人员卡号时，需确保设置的发卡类型与实际使用的发卡器类型一致，否则可能无法自动读取卡号。系统默认发卡器类型为 IC 卡。

步骤1 打开门禁方案，在主页单击“人事管理”或在门禁向导单击.

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 打开门禁方案，在主页单击“人事管理”或在门禁向导单击.

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

- 每个人员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 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 打开门禁方案，在主页单击“人事管理”或在门禁向导单击.

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 读卡卡号

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

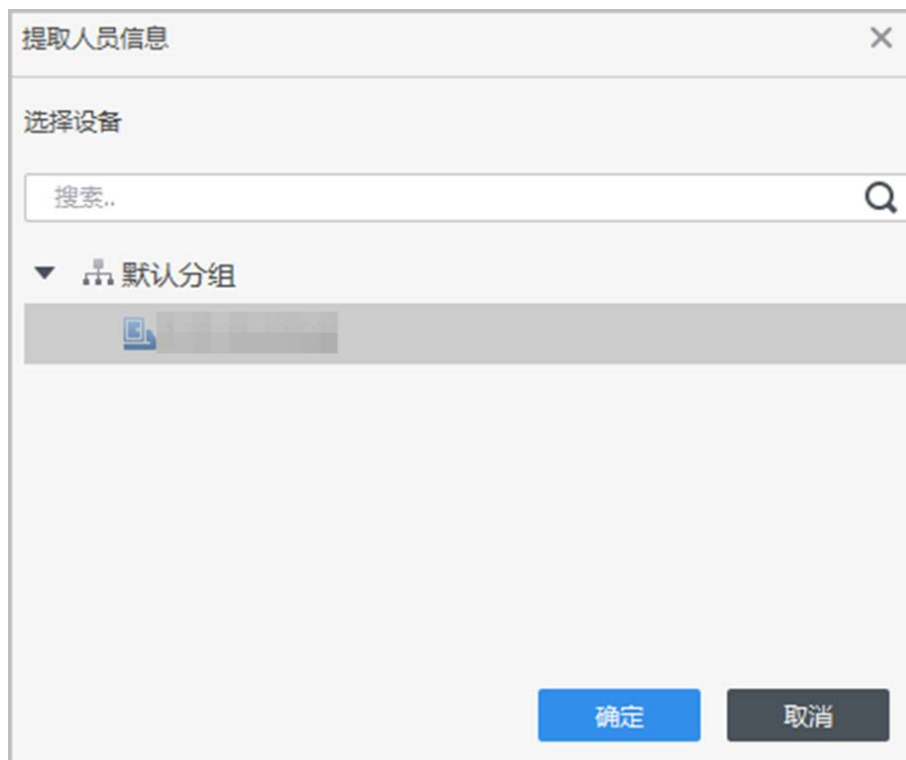
4.1.3.3 从设备中提取人员信息

步骤1 打开门禁方案，在主页单击“人事管理”页签或在门禁向导单击 .

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



序号	编号	名称	卡号	人员类型	部门	指纹数
1	888	888	159F82E9	普通用户		0

4.1.3.4 从本地导入人员


步骤1 打开门禁方案，在主页单击“人事管理”页签或在门禁向导单击.

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 打开门禁方案，在主页单击“人事管理”或在门禁向导单击.

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: * ●●●●●●

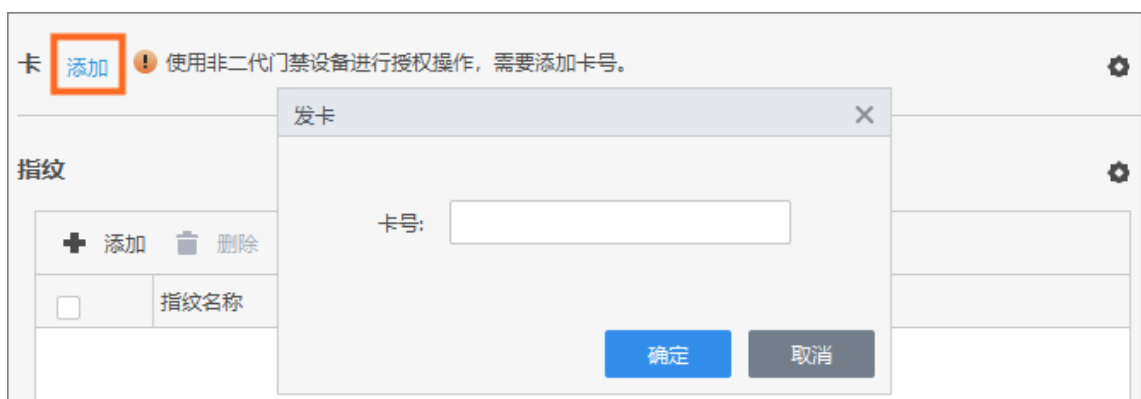
确定 取消

- 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



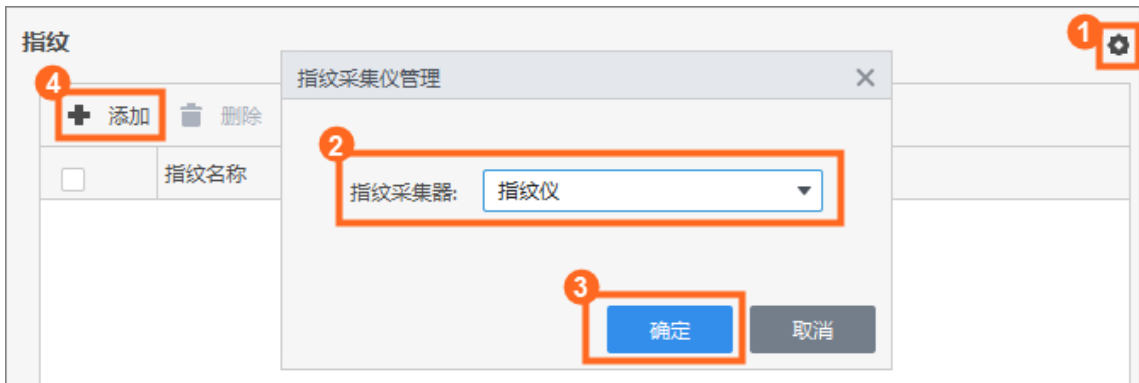
- 录入人员指纹。

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”。

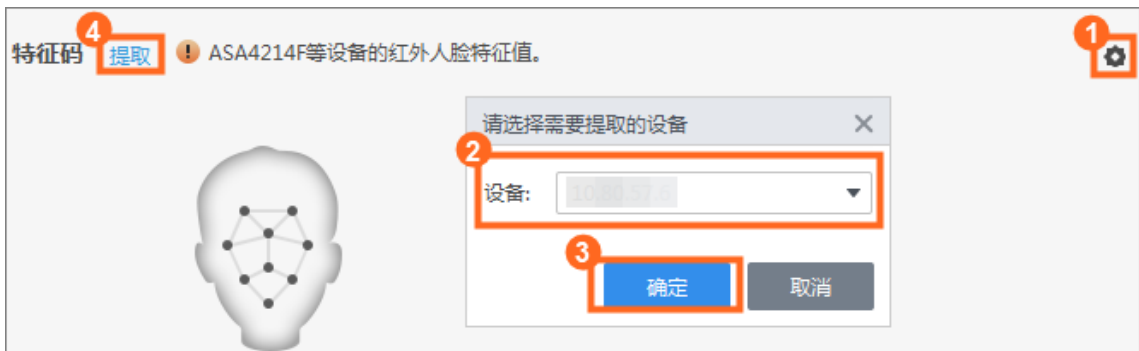
图4-13 录入人员指纹



- 上传人员特征码（仅部分设备支持）。

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 打开门禁方案，在主页单击“人事管理”页签或在门禁向导单击.

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

为人员设置门禁通行权限，分为绑定用户权限组和绑定设备两种方式。

- 步骤1 打开门禁方案，在主页单击“人事管理”或在门禁向导单击.
- 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门禁的通行权限。
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门禁的通行权限。

4.2.1 新增权限组

将一个或多个门禁设备设置为一个门禁权限组。




- 步骤1 打开门禁方案，在主页单击“人事管理”或在门禁向导单击.
- 步骤2 在左侧导航栏单击.
- 步骤3 单击，在弹出的对话框输入权限组名称，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门禁权限。

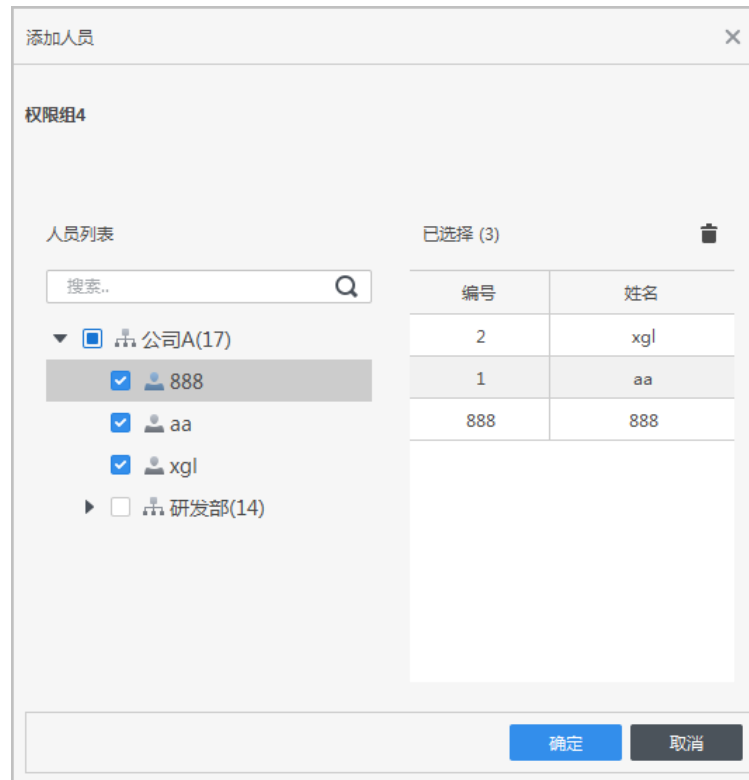
步骤1 打开门禁方案，在主页单击“人事管理”或在门禁向导单击.

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 打开门禁方案，在主页单击“人事管理”或在门禁向导单击.

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 打开门禁方案，在主页单击“人事管理”或在门禁向导单击.

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 dialog box titled "手动提取" (Manual Extraction) contains the following elements:

- 提取日期:** A date range selector showing "2020/10/30 0:00:00" to "2020/11/30 23:59:59".
- 重复数据覆盖:** A checkbox that is checked, indicating that duplicate data will be overwritten.
- 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 门禁配置

5.1 创建时间模板



如果系统提供的时间模板无法满足您的需求，您可以创建满足需求的时间模板。通过时间模板设置允许通过门禁的时间。系统默认提供 4 种时间模板。

说明

系统默认提供的时间模板，不支持修改。

创建时间模板的操作步骤如下：

步骤1 打开门禁方案。

步骤2 在主页单击“门禁配置”页签，然后在左侧导航树单击或在门禁向导单击.

步骤3 在时间模板界面单击“添加”。

步骤4 设置时间模板。

1. 在弹出的界面设置模板名称。
2. 单击“周计划”页签。
3. 设置周一～周日允许通过指定门禁的时间。支持如下任意一种设置方式。



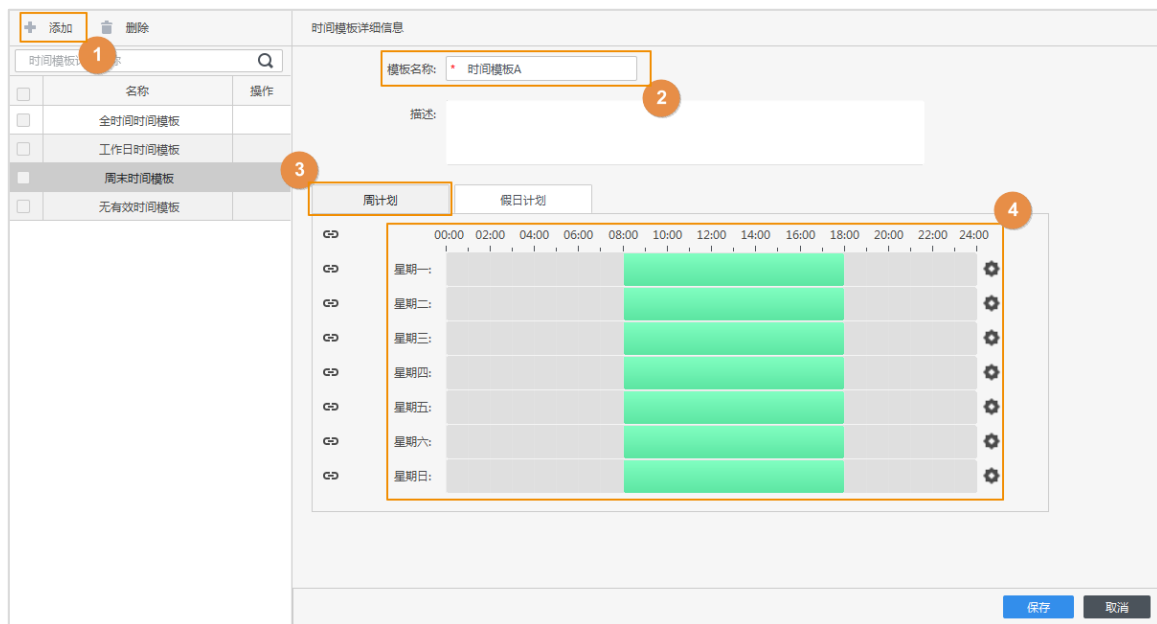
- ◇ 方式一：光标移动到待设置灰色区域，光标变为，滑动光标，对应时间段显示绿色，该时间段允许通过指定门禁，如果要设置某时间段禁止通过门禁，则将光标移动到对应绿色时间段，光标变为，滑动该光标，绿色修改为灰色，则该时间段不允许通过门禁。

图5-1 设置周一～周日允许通过指定门禁的时间（方式一）




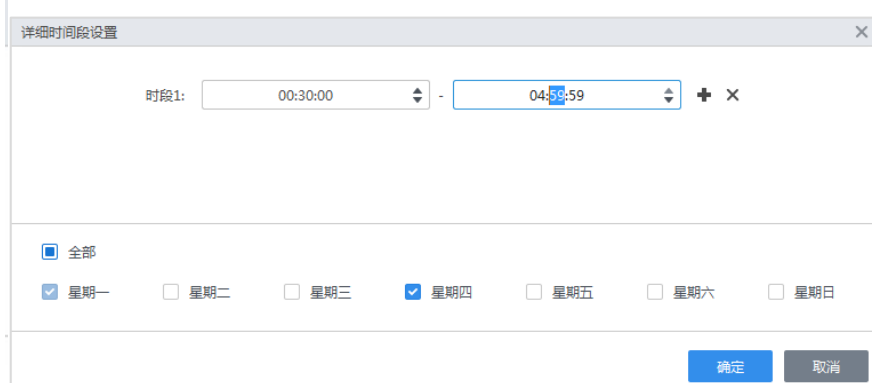
- ◇ 方式二：单击时间条右侧的 ，在弹出的对话框中设置时间段，在下方选择需要使用该时间段的星期，单击“确定”。

图5-2 设置周一～周日允许通过指定门禁的时间（方式二）



详细时间段设置

时段1: 00:30:00 - 04:59:59

☒ 全部

☒ 星期一 ☐ 星期二 ☐ 星期三 ☒ 星期四 ☐ 星期五 ☐ 星期六 ☐ 星期日

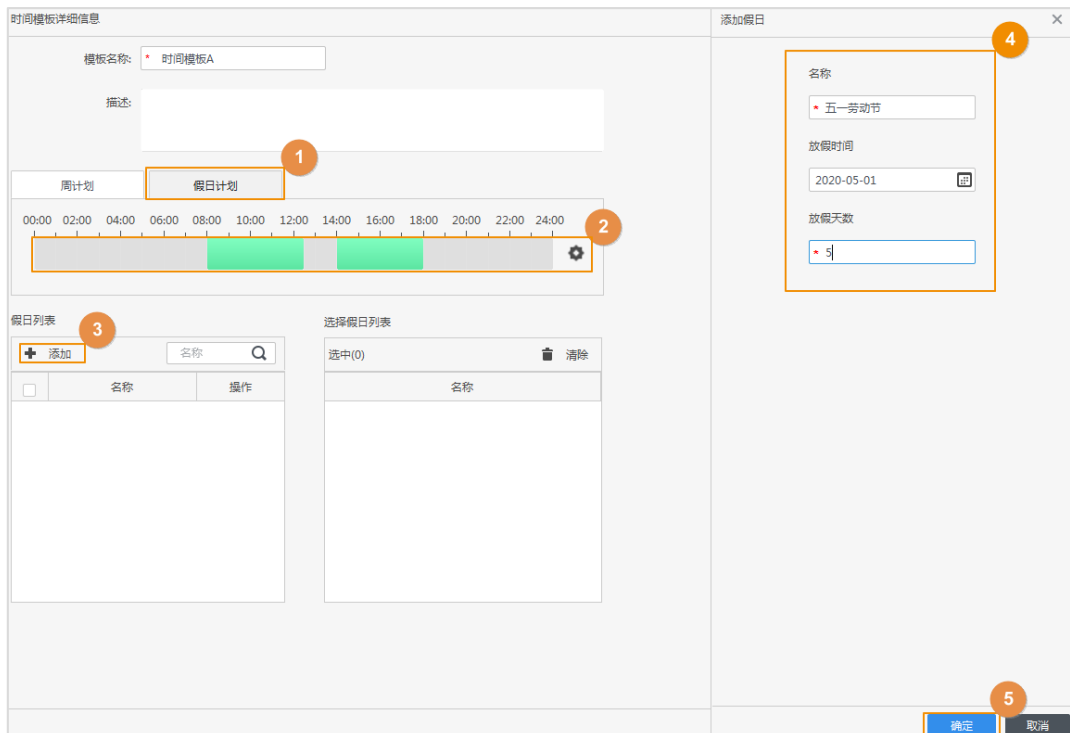
确定 取消

4. 设置假日计划。单击“假日计划”页签，在时间栏设置允许通过指定门禁的时间，单击“添加”，在右侧界面填写假日信息，单击“确定”。在假日列表选择需要的假日，单击“保存”。

说明

假日计划优先级高于周计划，如果周计划和假日计划门禁通行权限矛盾，按假日计划执行。

图5-3 设置假日计划（1）



时间模板详细信息

模板名称: 时间模板A

描述:

周计划 假日计划

00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00

假日列表

+ 添加

名称

选择假日列表

选中(0)

清除

名称

添加假日

名称: 五一劳动节

放假时间: 2020-05-01

放假天数: 1

确定 取消

图5-4 设置假日计划（2）

时间模板详细信息

模板名称: 时间模板A

描述:

周计划

假日计划

00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00

假日列表

+ 添加

名称

操作

6

五一劳动节

选择假日列表

选中(1)

清除

名称

五一劳动节

保存

取消

5.2 高级配置

5.2.1 配置首卡开门

每天只有设定的首卡刷卡开门后，其他非首卡刷卡才能开门。可以设定多张卡为首卡，任何一张刷卡开门后，其他非首卡刷卡都能开门。



说明

首卡人员的人员类型只能为普通用户，人员类型在添加人员时设置，操作请参见“4.1.3 添加人员”。

前提条件

已赋予首卡持有人员门禁的通行权限，详细介绍请参见“4.1.5 配置人员权限”。

操作步骤


- 步骤1 打开门禁方案，在主页单击“门禁配置”页签。
- 步骤2 在左侧导航树单击，单击“首卡开门”页签。
- 步骤3 单击“添加”，配置首卡开门参数，单击“保存”。

图5-5 首卡开门配置

首卡开门设置

门: 门 1

时段: 全时间时间模板

状态: 正常

选择人员

下拉选择

搜索..

<input type="checkbox"/>	编号	名称
<input checked="" type="checkbox"/>	11	11
<input type="checkbox"/>	22	22
<input type="checkbox"/>	33	33

已选择(1)

清除



编号	名称	操作
11	11	

保存

取消

表 4-60 首卡开门参数说明

参数	说明
门	选择需要配置首卡开门的门禁通道。
时间模板	选择的时间模板的时间段内首卡开门生效。
状态	设置首卡开门后门的状态。
人员	选择首卡持有的人员。支持选择多人，其中任何一个人刷开即完成首卡开门。

步骤4 （可选）单击 ，启用规则，图标显示为 .

如果规则已经启用，请忽略此步骤。新增规则默认启用。

5.2.2 配置多人开门

某个门禁通道需要多组人按照组的先后顺序刷卡才可以开门。

- 一个人员组最多 50 人。
- 启用多卡开门的门禁通道，最多支持 4 组人同时在场验证，总人数最多 200 人，有效总人数最多 5 人。

说明

- 首卡开门优先级高于多卡开门，同时开启规则，系统先执行首卡开门规则。
- 首卡开门人员不建议加入多卡开门人员组。首卡人员刷卡，系统识别为首卡开门规则。
- 人员组中人员的类型不能为 VIP 用户和巡逻用户，人员类型在添加人员时设置，详细操作请参见“4.1.3 添加人员”。

前提条件

已赋予开门人员门禁的通行权限，详细介绍请参见“4.1.5 配置人员权限”。

操作步骤

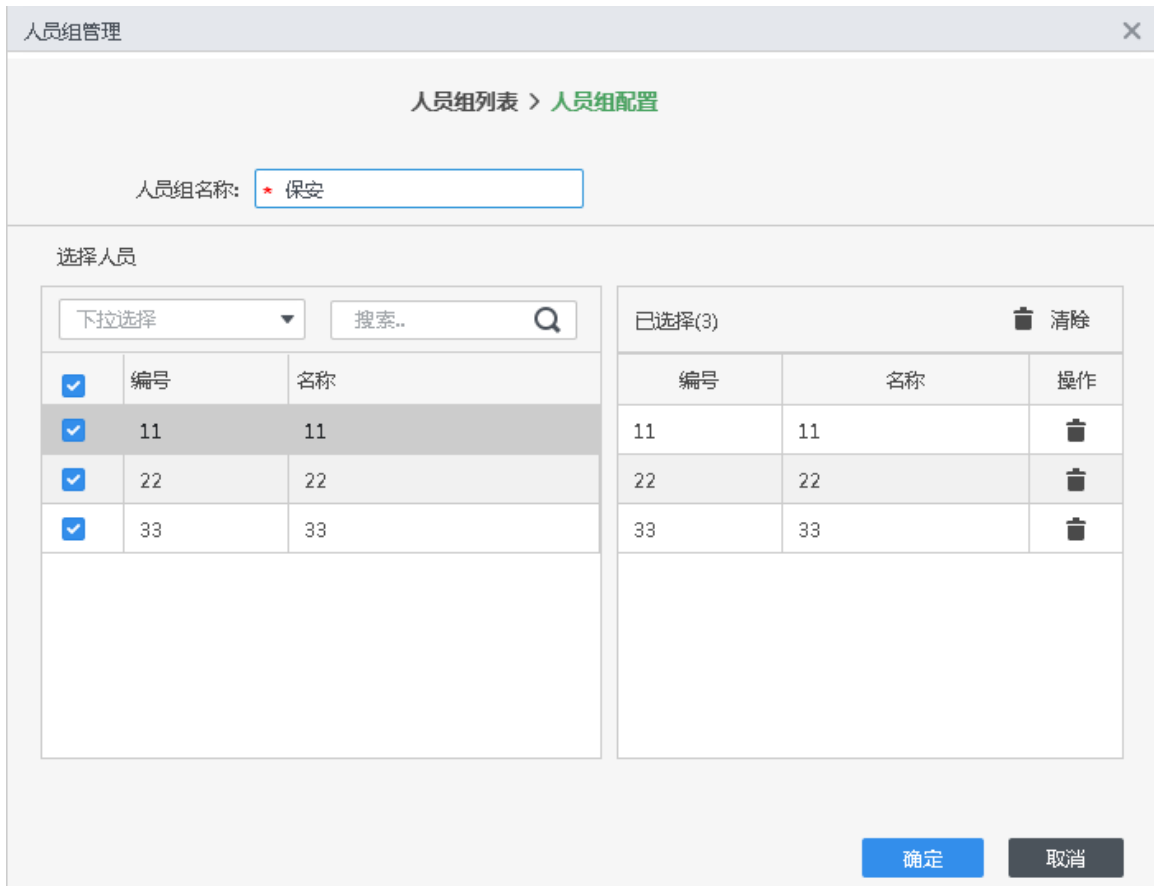
步骤1 打开门禁方案，在主页单击“门禁配置”页签。

步骤2 在左侧导航树单击，单击“多人开门”页签。

步骤3 添加人员组。

1. 单击“人员组”。
2. 单击“添加”，设置“人员组名称”，在人员列表中选择人员，最多选择 50 人。

图5-6 配置人员组






人员组管理

人员组列表 > 人员组配置


人员组名称: * 保安

选择人员

下拉选择	搜索..	已选择(3)	清除
<input checked="" type="checkbox"/>	编号	名称	
<input checked="" type="checkbox"/>	11	11	
<input checked="" type="checkbox"/>	22	22	
<input checked="" type="checkbox"/>	33	33	

确定 取消



3. 单击“确定”。

4. 单击“人员组管理”界面右上角，退出配置界面。

步骤4 配置多卡开门。

1. 单击“添加”。

2. 选择需要设置多卡开门的“门”和人员组，人员组最多选择 4 个。

3. 填写每组到场的有效人数和开门方式，单击或调整每组开门的先后顺序。

有效人数指每组必须到场刷门禁的人数。以图 5-7 配置举例，必须人事组任意两位人员刷卡，然后保安组任意 1 位人员刷卡，才能开门。

图5-7 添加多卡开门（1）

多人开门设置

门: nnn

人员组列表

搜索..

<input checked="" type="checkbox"/>	人员组名称	人数
<input checked="" type="checkbox"/>	保安	3
<input checked="" type="checkbox"/>	人事	2

选中(2)



清除

人员组名称	人数	有效人数	开门方式	操作
人事	2	2	刷卡	↑ ↓
保安	3	1	刷卡	↑ ↓

确定

取消

4. 单击“确定”。


步骤5 （可选）单击，启用规则，图标显示为.

如果规则已经启用，请忽略此步骤。新增规则默认启用。

5.2.3 配置反潜回

反潜回是指验证的人员，从某个门组进，从指定门组出，必须一进一出严格对应。进门未验证，尾随别人进来，出门验证时系统验证不通过。如果出门未验证，尾随别人出去，再验证进入时系统验证不通过。

步骤1 打开门禁方案，在主页单击“门禁配置”页签。

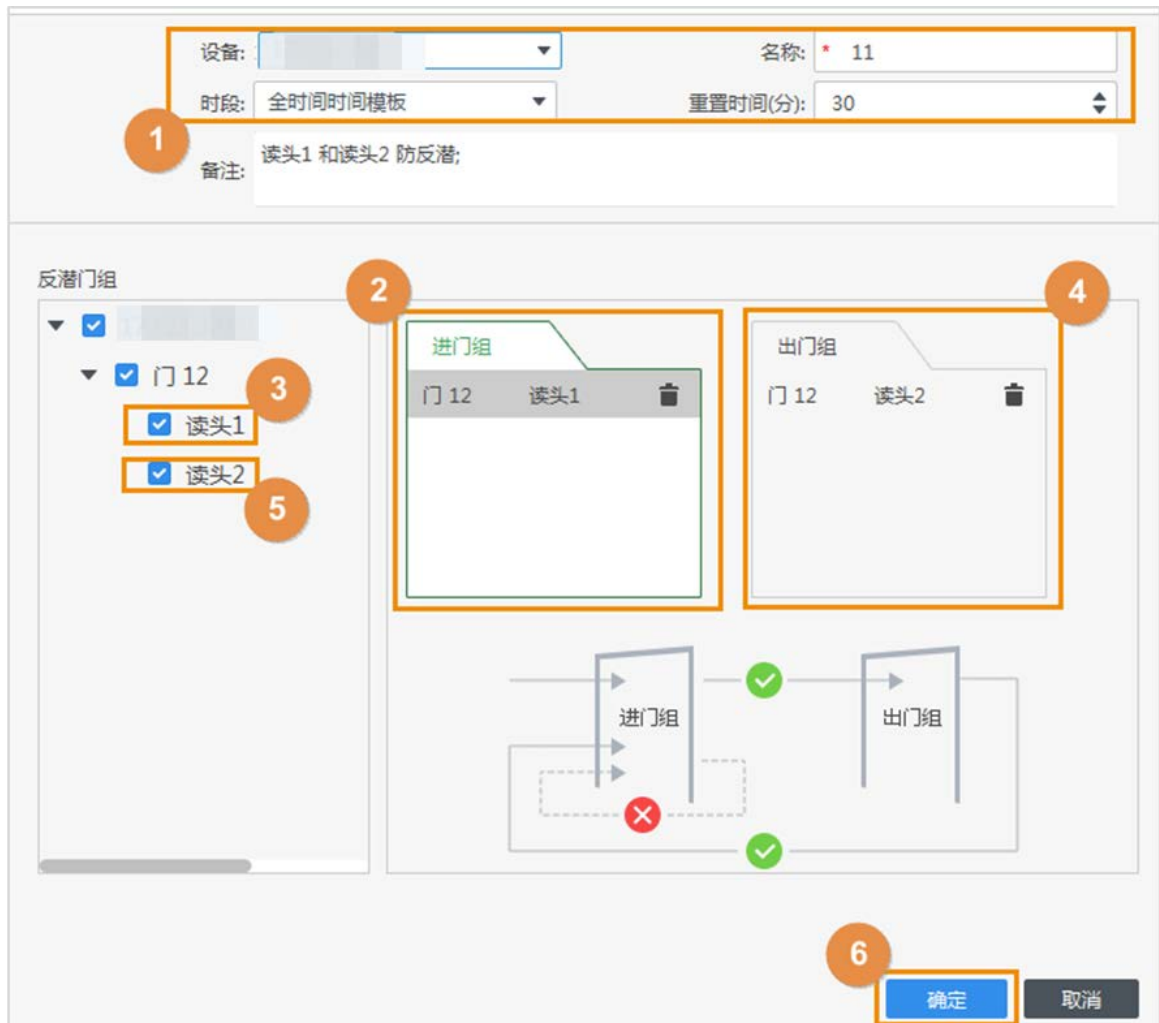
步骤2 在左侧导航树单击，单击“多人开门”页签，单击“添加”。

步骤3 配置反潜回参数。


- 在“设备”下拉列表框选择门禁设备，并设置设备名称；在“时段”下拉列表框选择要应用配置时间对应的的时间模板；在“重置时间”栏设置验证进门后触发防反潜报警的时间，例如设置为 30 分钟，当人员验证进门且没有验证出门，30 分钟内如果再次验证进门，则触发防反潜报警；如果人员验证进门且有验证出门，则 30 分钟内再次验证进门，不会触发防反潜报警。
- 单击“进门组”。
- 在组织树设置进门设备读头。
- 单击“出门组”。

5. 在组织树设置出门设备读头。
6. 单击“确定”，完成设置。

图5-8 配置反潜回



步骤4 配置防反潜报警。配置后，一旦发生反潜，将上报消息到系统。在“门禁管理”的事件列表，可以查看该事件。


1. 在主页单击“事件配置”。
在组织树选择门禁
2. 选择“异常事件 > 防反潜模式”。
3. 单击“防反潜模式”右侧的 ☐，开启防反潜报警。
4. 按照实际需求配置防反潜报警联动，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。

5.2.4 配置多门互锁

多门互锁实现组内互锁，即门组的一个门禁通道开启时，该门组的其它门禁通道都关闭。当要开启一个门禁通道时，其它对应的门禁通道必须关闭，否则无法开门。门组之间互不影响。

1 个门禁设备配置 2 个门组，每个门组最多添加 4 个门。

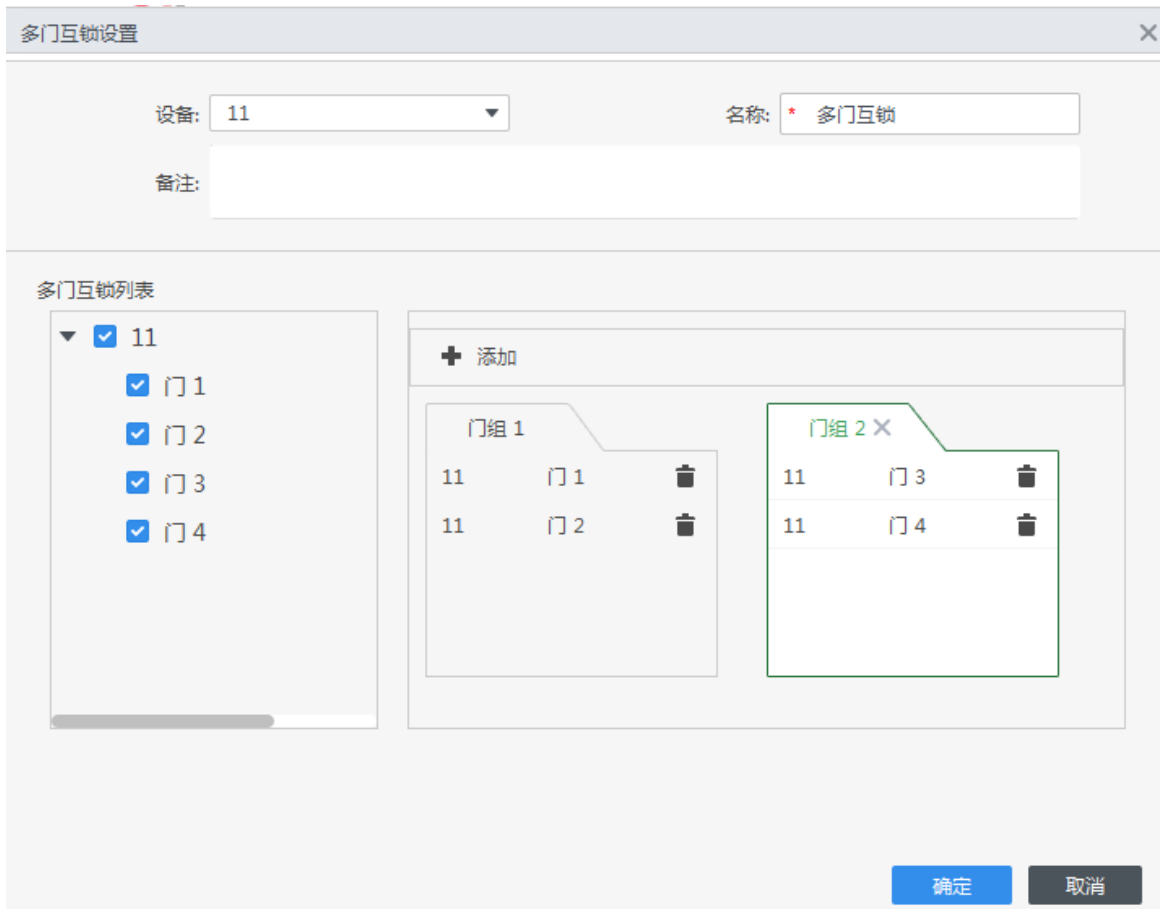
步骤1 打开门禁方案，在主页单击“门禁配置”页签。



步骤2 在左侧导航树单击 ，单击“多门互锁”页签，单击“添加”。

步骤3 配置多门互锁参数。

1. 在“设备”下拉列表框选择需要设置多门互锁的设备。
2. 在“名称”文本框自定义多门互锁规则名称。
3. 连续两次单击“添加”。
添加 2 个门组。
4. 添加门禁到 2 个门组。单击门组，在门禁组织树选择需要添加到该门组的门禁。
门禁自动添加到门组。
5. 单击“确定”。

图5-9 多门互锁配置



步骤4 （可选）单击 ，启用规则，图标显示为 。


如果规则已经启用，请忽略此步骤。新增规则默认启用。

5.3 门禁配置

通过门禁配置，修改门禁名称，远程配置该门禁进门和出门读头、常开和常闭时段等。

说明

设备类型不同支持的配置功能略有不同，请以实际界面设置为准。

步骤1 打开门禁方案，在主页单击“门禁配置”页签，在左侧导航树单击.

步骤2 在组织树选择要配置的门禁，在右侧配置门禁信息。

图5-10 门禁配置

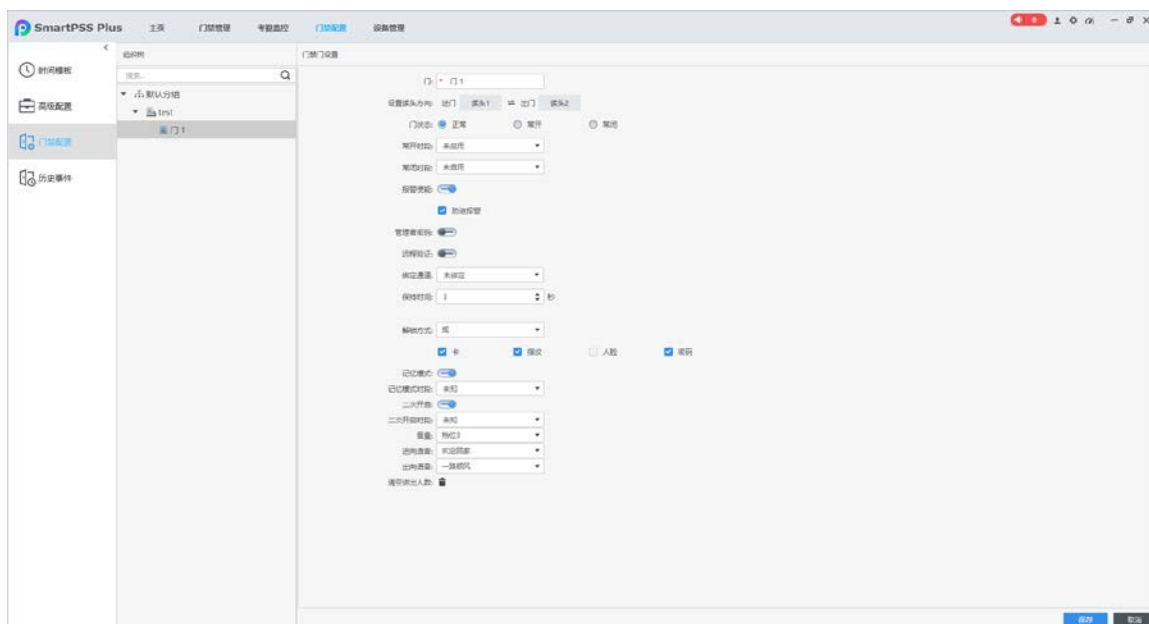








表5-1 门禁配置说明

项目	说明
门	设置门禁名称。设置后，该门禁显示设置的名称。
设置读头方向	单击  , 按照实际情况设置进门和出门的读头。
门状态	设置门禁状态。设置后，状态将下发到相应门禁。
常开时段	设置“门状态”为常开后，需选择门常开时间对应的时间模板，在时间模板对应的时间里该门禁处于常开状态。
常闭时段	设置“门状态”为常闭后，选择门常闭时间对应的时间模板，在时间模板对应的时间里该门禁处于常闭状态。
报警使能	报警总开关。开启报警使能，且配置事件报警后，一旦发生相应的事件报警，会发送报警消息。
门磁	门磁主要用于物理检测门禁的真实开闭状态。如需使用闯入和门超时未关报警功能，需要开启门磁功能。
管理员密码	开启管理员密码，并在弹出的文本框设置管理员密码。设置管理员密码后，在门禁界面只需输入管理员密码，即可开门。
远程验证	开启远程验证并选择时间模板后，时间模板设置的生效时间内有人在门禁通过刷卡等申请开门，需要系统端确认，确认通过后门禁才开门。
绑定通道	设置门禁联动的视频通道。设置后，预览门禁视频时，将显示联动视频通道的实时视频。
保持时间	设置开门后门的持续打开时间。超过该时间，门会自动关闭。
超时时间	设置门超时未关报警时间。例如设置为 60 秒，则超过 60 秒未关门，将上报报警消息。

项目	说明
解锁方式	<p>请按实际需求配置开门方式，支持如下任意一种开门方式。</p> <ul style="list-style-type: none"> 选择“和”，并在下方选择解锁方式，则需同时满足配置的方式，才能开门。 选择“或”，并在下方选择解锁方式，则满足配置的任意一种方式，均能开门。 选择“按时段开锁”，单击，在弹出的对话框选择时间，并配置该时间的开门方式。完成配置后，该时间内必须满足配置的方式才能开门。 选择“人证解锁方式”，并选择具体解锁方式，则需满足配置的方式，才能开门。 <p>人证对比和身份证的含义如下：</p> <ul style="list-style-type: none"> 人证对比：采集到的人脸与身份证中照片比对。 身份证：采集的身份证号码与系统中的身份证号码比对。
<ul style="list-style-type: none"> 记忆模式 记忆模式时段 	<p>仅部分门禁支持开启记忆功能。</p> <p>开启“记忆模式”，在“记忆模式时段”配置生效时间段，则连续多次刷卡后允许连续多人通行，适用于短时间人流量较大的场景。</p> <p> 说明</p> <ul style="list-style-type: none"> 如果连续多人授权通行，其中一名人员未在 5s 内进入通道开始通行，或通行超时滞留，则门翼关闭，未通过的人数清零，需要重新多次刷卡后允许连续多人通行。 在记忆功能打开的情况下，如果刷卡间隔时间超过设定的单人通行时间，则记忆功能不会被触发。 连续刷卡时，每两张卡的刷卡时间间隔必须长于门禁开门后的保持时间，否则按 1 张卡处理。建议每两张卡的刷卡时间间隔为 2s~5s。 <p>记忆功能最多支持 255 个人。</p>
<ul style="list-style-type: none"> 二次开启 二次开启时段 	<p>仅部分门禁支持二次开启功能。</p> <p>二次开启功能开启后，通行人员在非法闯入通行区域且触发闯入报警后，无需退出通行区域即可验证通行。</p>
音量	<p>设置音量档位，默认八个档位，档位一音量最小，档位八音量最大。</p>
进向语音/出向语音	<p>选择进向/出向语音，默认支持选择五种语音。</p>
清空进出人数	<p>单击，清空进出人数。清空后，门禁管理闸机设备进出人数显示为 0。</p>
广告配置	<p>单击，配置广告投放信息。支持上传 dav 格式的音视频文件及 png、jpg 格式的图片文件。</p> <ul style="list-style-type: none"> 循环播放：当设备检测到行人时，开始循环播放广告，直至行人离开时息屏。 一次播放：当设备检测到行人时，播放一次广告后息屏。 <p> 说明</p> <p>仅部分设备支持此功能。</p>

5.4 查询门历史事件


门历史事件包括系统端发生的历史事件和门设备端发生的历史事件。查看门历史事件之前，需要先提取门设备端的历史事件，从而确保查询到门的所有历史事件。

前提条件

请确保查询的人员已添加到系统。

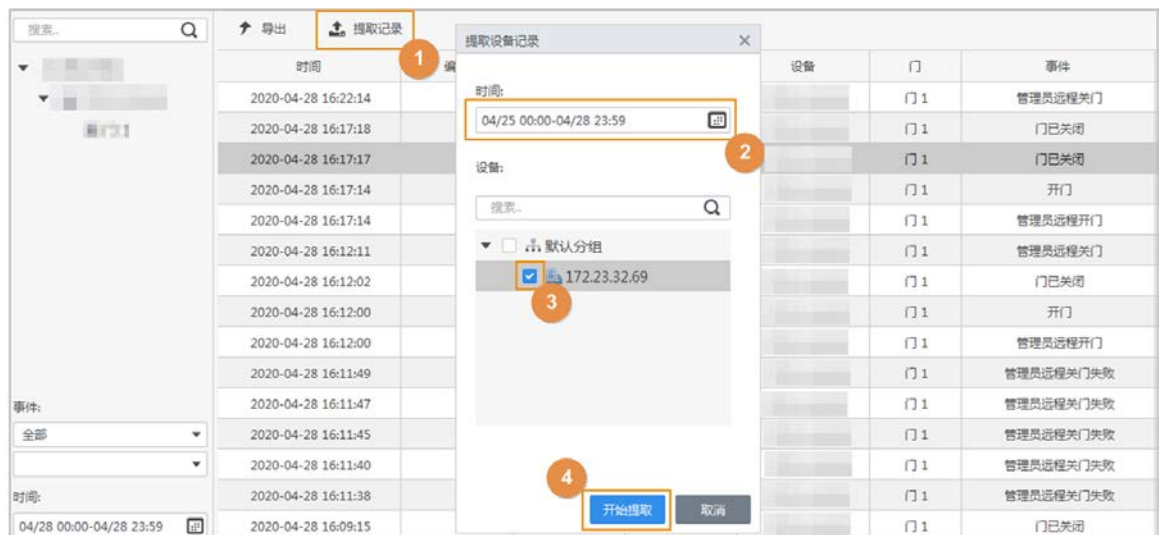
操作步骤

步骤1 打开门禁方案。

步骤2 在主页选择“门禁管理 > 历史事件”，或在“门禁配置”界面单击.

步骤3 提取门设备端的事件到本地。单击“提取记录”，在弹出的对话框设置提取时间段，在设备树选择门设备，单击“开始提取”。

图5-11 提取设备端的门事件



步骤4 在组织树设置筛选条件，单击“搜索”。
查询门设备上符合条件的所有门事件。

相关操作

单击“导出”，根据提示操作，将查询到的门事件保存到本地。

第6章 门禁管理

完成门禁业务配置后，即可通过系统远程监控门禁状态和操作门禁，例如开关门。

6.1 远程开关门

操作步骤


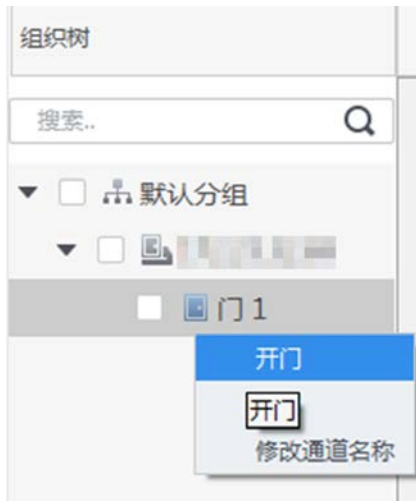
- 步骤1 打开门禁方案，在主页单击“门禁管理”页签或在门禁向导单击.
- 步骤2 在门禁管理界面远程开关门。
支持通过如下任意一种方式远程开关门。
- 方式一：在组织树选择要远程控制的门禁，右键选择“开门”或“关门”。

图6-1 远程开关门（方式一）



- 方式二：单击指定门禁右下角的和，远程控制该门禁的开和关。



说明

闸机设备支持统计进出人数功能。

图6-2 远程开关门（方式二）




相关操作

- 查看门禁信息。在“事件信息”列表，可以查看门禁的实时操作信息。重启系统后门禁信息会被清空。
- 筛选事件。在“事件信息”栏，选择需要查看的事件类型，事件列表显示该类型的事件，例如仅选择“报警”，则事件列表仅显示报警事件。
- 锁定事件刷新。在“事件信息”右侧单击，锁定事件列表，将无法查看到门禁的实时操作信息
- 删除所有事件。在“事件信息”右侧单击，清空事件列表的所有事件。

6.2 设置门常开或常关

设置门常开或门常关后，门将一直打开或一直关闭，此时无法手动开门或关门，需通过“恢复正常”将门恢复正常后，才能手动开门或关门。

步骤1 打开门禁方案，在主页单击“门禁管理”页签或在门禁向导单击.

步骤2 在门禁管理界面组织树选择要设置为常开或常关的门禁，单击“一键常闭”或“一键常开”。

图6-3 设置门常开或常关




6.3 查看门禁视频

查看门禁自带摄像头或联动的外部摄像机采集的视频。

- 当门禁自带摄像头，同时又联动外部摄像机时，查看的门禁视频是联动摄像机的视频。
- 当门禁自带摄像头，未联动外部摄像机时，查看的门禁视频是门禁自带摄像头的视频。
- 如果无法查看门禁视频，说明该门禁无摄像头，也未联动外部摄像机，请配置门禁联动外部摄像机。配置门禁联动外部摄像机的操作方法是，选择“门禁配置 > 门禁配置”，在门禁配置界面“绑定通道”下拉列表框配置需要联动的外部摄像机视频通道，详细介绍请参见“5.3 门禁配置”。

6.3.1 查看单个门禁实时视频

步骤1 打开门禁方案，在主页单击“门禁管理”页签或在门禁向导单击。



步骤2 在门禁管理界面单击“列表”，单击要查看视频的门禁右下角的。

图6-4 查看单个门禁实时视频



6.3.2 查看两个及以上门禁实时视频

步骤1 打开门禁方案，在主页单击“门禁管理”页签或在门禁向导单击。

步骤2 在门禁管理界面单击“视图”。

步骤3 查看门禁视频。

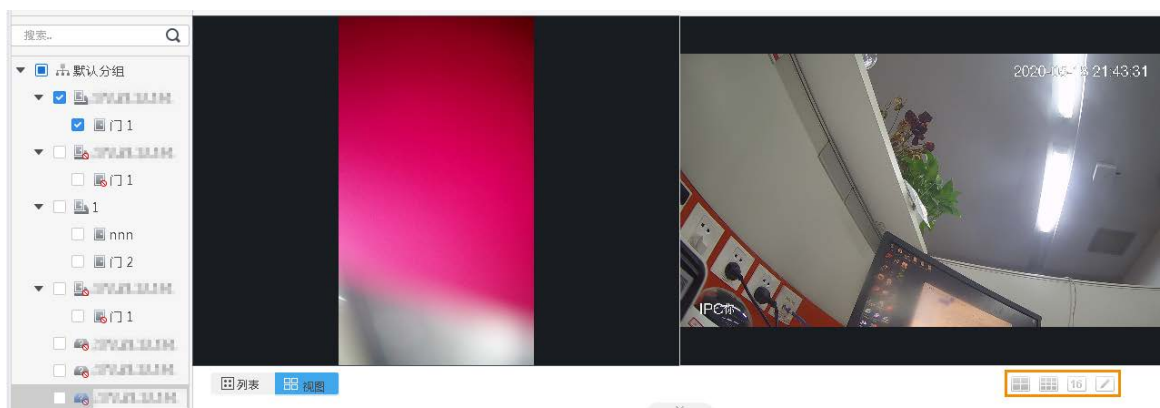
1. （可选）根据需要查看的视频数量设置窗口。例如需要查看 4 个门禁视频，则设置 4 个窗口。

通过窗口右下角的，设置窗口。

2. 在组织树将需要查看视频的门禁拖到显示视频的窗口，或单击显示视频的窗口，然后在组织树双击门禁。

查看门禁的视频。

图6-5 查看两个及以上门禁的视频



6.4 设置门禁点

将联动的支持人脸识别的智能设备（NVR、IPC、IVSS 等）设置为门禁点。设置后，设备人脸识别开门记录将上传到平台。


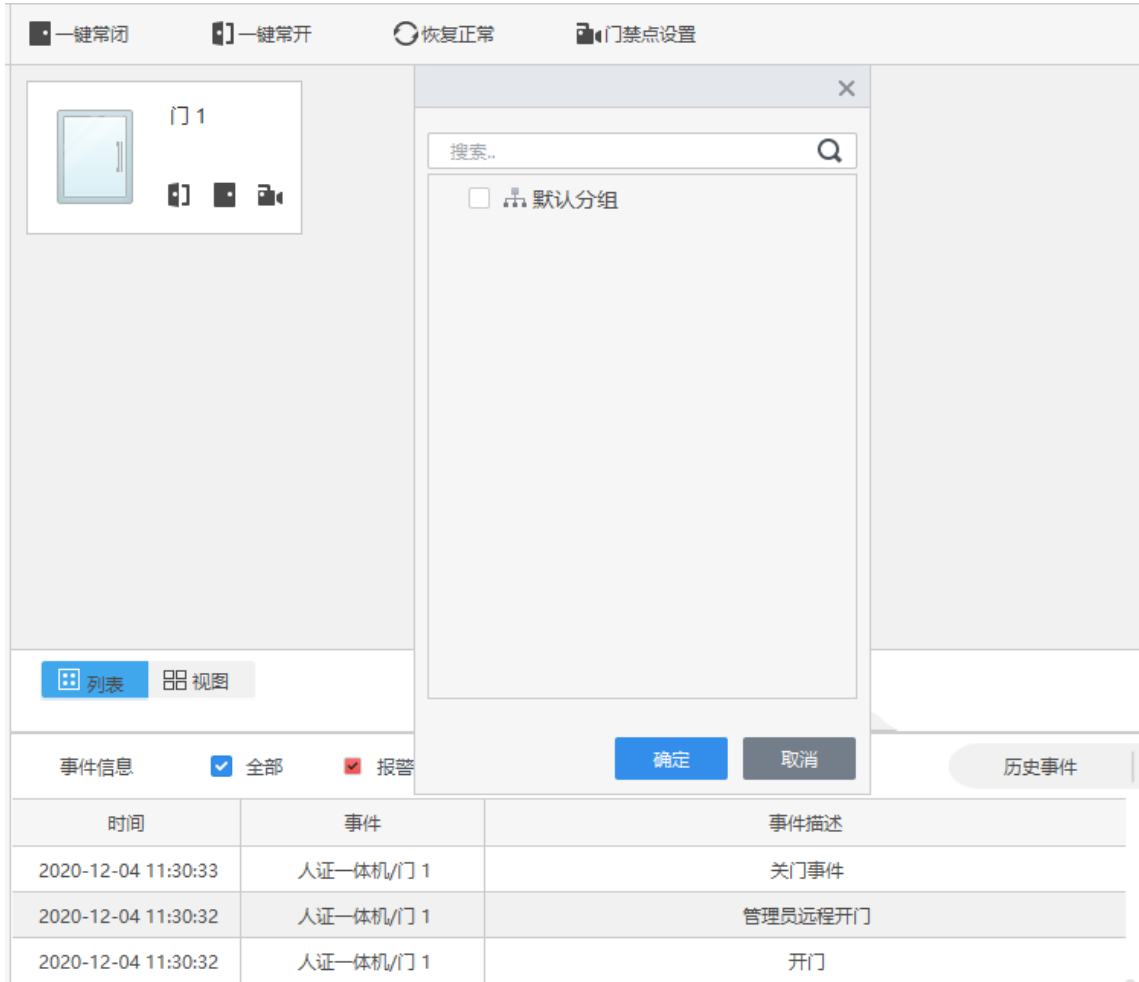
- 步骤1 打开门禁方案，在主页单击“门禁管理”页签或在门禁向导单击.
- 步骤2 单击“门禁点设置”。
- 步骤3 选择需要设置为门禁点的设备。

图6-6 设置门禁点



- 步骤4 单击“确定”。
- 在下方事件列表中可查看已添加门禁点的设备事件信息。

6.5 查看门禁详情

查看门禁 IP 地址、型号、状态、序列号和系统版本号等。


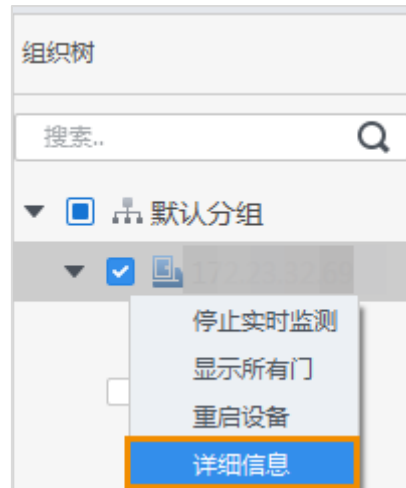
- 步骤1 打开门禁方案，在主页单击“门禁管理”页签或在门禁向导单击.
- 步骤2 在门禁管理界面组织树单击要查看详细信息的门禁，在右键菜单栏选择“详细信息”，查看该门禁详情。

图6-7 查看门禁详细信息



6.6 重启门禁

支持通过系统远程重启门禁。


- 步骤1 打开门禁方案，在主页单击“门禁管理”页签或在门禁向导单击.
- 步骤2 在门禁管理界面组织树单击要查看详细信息的门禁，在右键菜单栏选择“重启设备”，根据提示重启门禁。

图6-8 查看门禁详细信息



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。

免责声明

- 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：

3. 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。

4. 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。

5. 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。

6. 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。

7. 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。

8. 使能 HTTPS

建议您开启 HTTPS，通过安全的通道访问 Web 服务。

9. 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。

10. 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。

11. 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。

12. 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。

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。

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