ACSConfig

（Windows 版本）

使用说明书

V1.0.3

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。

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

- 产品请以实物为准，说明书仅供参考。
- 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。
- 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。

网络安全建议

保障设备基本网络安全的必须措施：

1. 修改出厂默认密码并使用强密码

没有更改出厂默认密码或使用弱密码的设备是最容易被“黑”的。建议用户必须修改默认密码，并尽可能使用强密码（最少有 8 个字符，包括大写、小写、数字和符号）。

2. 更新固件

按科技行业的标准作业规范，NVR、DVR 和 IP 摄像机的固件应该要更新到最新版本，以保证设备享有最新的功能和安全性。

以下建议可以增强设备的网络安全程度：

1. 定期修改密码

定期修改登录凭证可以确保获得授权的用户才能登录设备。

2. 更改默认 HTTP 和 TCP 端口

- 更改设备的默认 HTTP 和 TCP 端口这两个端口是用来进行远程通讯和视频浏览的。
- 这两个端口可以设置成 1025～65535 间的任意数字。更改默认端口后，减小了被入侵者猜到你使用哪些端口的风险。

3. 使能 HTTPS/SSL 加密

设置一个 SSL 证书来使能 HTTPS 加密传输。使前端设备与录像设备间的信息传输被全部加密。

4. 使能 IP 过滤

使能 IP 过滤后，只有指定 IP 地址的设备才能访问系统。

5. 更改 ONVIF 密码

部分老版本的 IP 摄像机固件，系统的主密码更改后，ONVIF 密码不会自动跟着更改。你须要更新摄像机的固件或者手动更新 ONVIF 密码。

6. 只转发必须使用的端口

- 只转发必须使用的网络端口。避免转发一段很长的端口区。不要把设备的 IP 地址设置成 DMZ。
- 如果摄像机是连接到本地的 NVR，你不需要为每一台摄像机转发端口，只有 NVR 的端口需要被转发。

7. 关闭 SmartPSS 的自动登录功能

如果你使用 SmartPSS 来监控你的系统而你的电脑是有多个用户，请必须把自动登录功能关闭。增加一道防线来防止未经授权的人访问系统。

8. 在 SmartPSS 上使用不同于其他设备的用户名和密码

万一你的社交媒体账户，银行，电邮等账户信息被泄漏，获得这些账户信息的人也无法入侵你的视频监控系统。

9. 限制普通帐户的权限

如果你的系统是为多个用户服务的，请确保每一个用户只获得它的作业中必须的权限。

10. UPnP

- 启用 UPnP 协议以后，路由器将会自动将内网端口进行映射。从功能上来说，这是方便用户使用，但是却会导致系统自动的转发相应端口的数据，从而导致本应该受限的数据被他人窃取。
- 如果已在路由器上手工打开了 HTTP 和 TCP 端口映射，我们强烈建议您关闭此功能。在实际

的使用场景中，我们强烈建议您不开启此功能。

11.SNMP

如果您不使用 SNMP 功能，我们强烈建议您关闭此功能。SNMP 功能限于以测试为目的的临时使用。

12.组播

组播技术适用于将视频数据在多个视频存储设备中进行传递的技术手段。当前为止尚未发现有过任何涉及组播技术的已知漏洞，但是如果您没有使用这个特性，我们建议您将网络中的组播功能关闭。

13.检查日志

如果您想知道您的设备是否安全，可以通过检查日志来发现一些异常的访问操作。设备日志将会告知您哪个 IP 地址曾经尝试过登录或者用户做过何种操作。

14.对您的设备进行物理保护

为了您的设备安全，我们强烈建议您对设备进行物理保护，防止未经授权的物理操作。我们建议您将设备放在有锁的房间内，并且放在有锁的机柜，配合有锁的盒子。

15.强烈建议您使用 PoE 的方式连接 IP 摄像机和 NVR

使用 PoE 方式连接到 NVR 的 IP 摄像机，将会与其它网络隔离，使其不能被直接访问到。

16.对 NVR 和 IP 摄像机进行网络隔离

我们建议将您的 NVR 和 IP 摄像机与您的电脑网络进行隔离。这将会保护您的电脑网络中的未尽授权的用户没有机会访问到这些设备。

概述

本文档详细描述 ACSConfig 的功能和界面操作等。

符号约定

在本文中可能出现下列标志，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。
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

编号	版本号	修订内容	发布日期
1	V1.0.0	首次发布。	2016.7.8
2	V1.0.1	删除“安装与卸载”章节。	2016.11.18
3	V1.0.2	新增初始化设备、修改密码和重置密码。	2017.5.31
4	V1.0.3	1、 新增隐私保护提醒。 2、 更新关于本文档。	2018.5.3

目录

法律声明 ..... **I**
网络安全建议 ..... **II**
前言 ..... **IV**
1 简介 **1**
1.1 概述 1
1.2 主界面 1
2 日常操作 **3**
2.1 配置系统参数 3
2.2 添加设备 3
2.2.1 搜索添加 4
2.2.2 通过模板添加 4
2.3 初始化设备 7
2.4 修改 IP 9
2.4.1 单个修改 9
2.4.2 批量修改 10
2.5 配置系统信息 11
2.5.1 校准时间 11
2.5.2 重启设备 12
2.5.3 恢复默认 13
2.5.4 修改密码 15
2.5.5 重置密码 16
2.6 升级设备 22
2.6.1 单个升级 22
2.6.2 批量升级 23

1 简介

1.1 概述

ACSConfig 主要用于配置和维护门禁设备，可以进行如下操作：

- 修改设备的 IP 地址。
- 校准设备时间、重启设备、恢复系统默认、修改和重置设备密码。
- 升级设备。

1.2 主界面

打开 ACSConfig，ACSConfig 的主界面如图 1-1 所示，详细说明请参见表 1-1。

说明

- 启动工具后，工具会自动按照“搜索设置”里选择的网段搜索设备。
- 工具安装完成后首次启动时“搜索设置”里默认选择“当前网段搜索”。

图1-1 ACSConfig 主界面

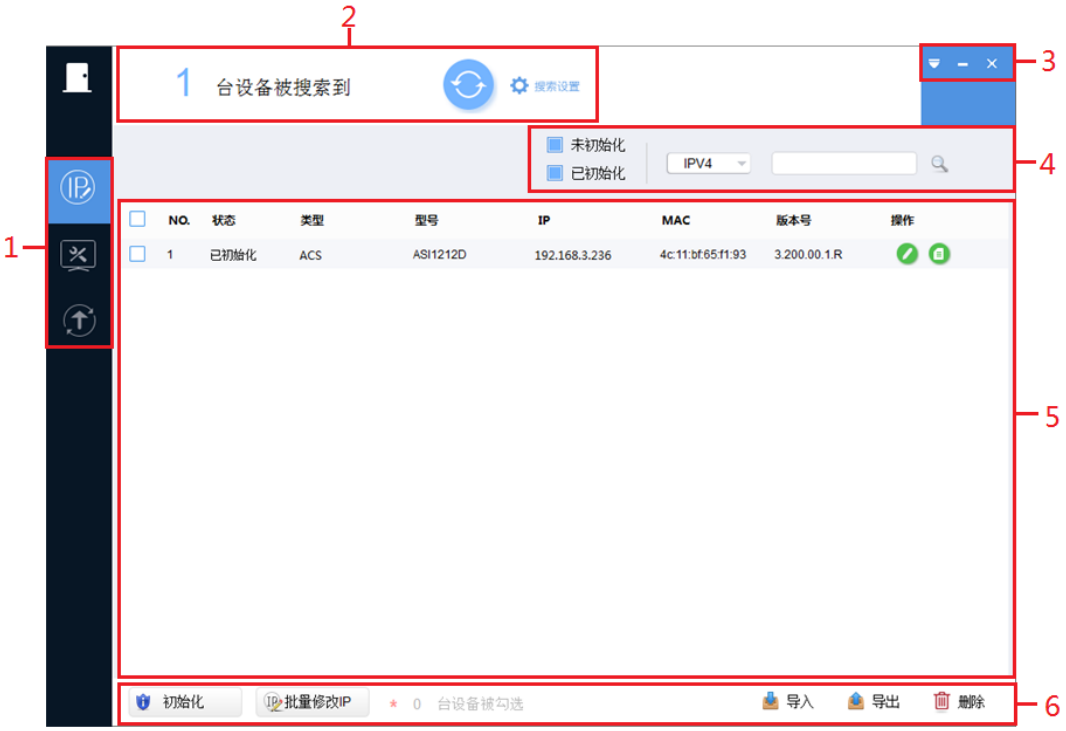
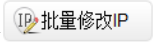


表1-1 主界面介绍

序号	功能	说明
1	菜单栏	包括修改 IP、系统配置和升级页签。 ● ：可以单个或者批量修改设备 IP。 ● ：可以设置设备系统时间、重启设备、恢复默认、修改密码和重置密码。 ● ：可以单个或者批量升级设备。
2	搜索设置	搜索当前网段设备。 单击 ，刷新搜索到的设备列表。
3	帮助图标	可以查看帮助文档和软件版本信息、设置系统参数、最小化或者退出软件。 ● 单击 ，查看帮助文档和软件版本信息、设置搜索备用端口和升级。 ● 单击 ，最小化软件。 ● 单击 ，退出软件。
4	筛选	通过选择设备类型、初始化状态、设备 IP（IPV4 或者 IPV6）快速筛选设备，也可以通过输入搜索条件（类型、IP、型号、MAC 地址、版本号等）筛选设备。
5	设备列表	显示搜索到的设备和设备信息，包括类型、型号、IP、MAC 和版本号。在“操作”列可进行如下操作： ● 单击 ，修改设备 IP。 ● 单击 ，查看设备信息。 说明 不支持在 IPV6 地址下修改 IP 和查看信息列表功能。
6	功能配置	包括初始化设备、批量修改设备 IP、导入设备、导出设备和删除设备的功能。 ● 初始化设备：选择设备，单击 ，对设备进行初始化操作。 ● 批量修改设备 IP：选择设备，单击  ，可以同时修改多个设备的 IP。 ● 导入设备：单击 ，通过模板可以批量导入设备。 ● 导出设备：选择设备，单击 ，导出选中的设备信息。 ● 删除设备：选择设备，单击 ，可以删除设备。

2 日常操作

2.1 配置系统参数

设置搜索设备的备用端口、升级设备时的升级超时时间和网络超时时间。

步骤1　在主界面单击，并选择“设置”。

系统弹出“设置”对话框，如图 2-1 所示。

图2-1 设置

步骤2　设置系统参数，详细参数说明请参见表 2-1。

表2-1 系统参数说明

参数	说明
广播搜索备用端口	搜索设备时使用的备用端口。 当使用默认广播搜索端口不能搜索到设备时，自动切换为备用端口搜索设备。
升级超时时间	设备升级时，单个设备的最长升级时间。 当设备升级的时间大于设置的值时，系统停止升级设备。
网络超时时间	设备升级时，网络连接的最大超时时间。 当设备升级的网络超时时间大于设置值时，系统停止升级设备。

步骤3　单击“确定”，完成配置。

2.2 添加设备

通过搜索或者模板导入批量添加设备，请根据实际情况选择合适的添加方式。

- 通过搜索添加当前网段的设备，具体操作请参见“2.2.1 搜索添加”。
- 当已有设备的模板数据时，可以通过模板导入设备，具体操作请参见“2.2.2 通过模板添加”。

注意

请确保设备和安装 ACSConfig 的 PC 间网络互通，否则 ACSConfig 无法搜索到设备。

2.2.1 搜索添加

通过搜索批量添加当前网段的设备。系统只支持搜索当前网段的设备。

步骤1　单击 搜索设置 。

系统显示“设置”界面，如图 2-2 所示。

图2-2 设置

步骤2　选择“当前网段搜索”，并设置“用户名”和“密码”。

说明

“用户名”和“密码”是修改 IP、配置系统参数信息和升级设备时登录设备的用户名和密码。

步骤3　单击“确定”。

系统开始搜索设备。

搜索完成后，系统显示搜索添加的设备。

说明

- 单击 ，刷新搜索到的设备列表。
- 通过设定筛选条件，可以在搜索结果中快速查找出符合条件的设备。
- 关闭工具时会保存设置的搜索条件，重新开启工具时会启用上次保存的设置。

2.2.2 通过模板添加

通过模板添加设备，可以快速将需要的设备添加到系统中。

说明

请确认 PC 已安装 Microsoft Excel 软件。

2.2.2.1 获取模板

手动填写模板文件或者将从系统中导出的设备信息文件作为模板文件。

- 填写模板文件的操作请参见“填写模板文件”。
- 导出设备信息的操作请参见“导出设备信息文件”。

说明

- 模板文件（设备导入模板.xls）必须使用 Excel 工具打开和编辑。
- 删除模板文件中的记录时，必须先选中对应行，右键选择“删除”，删除对应记录。

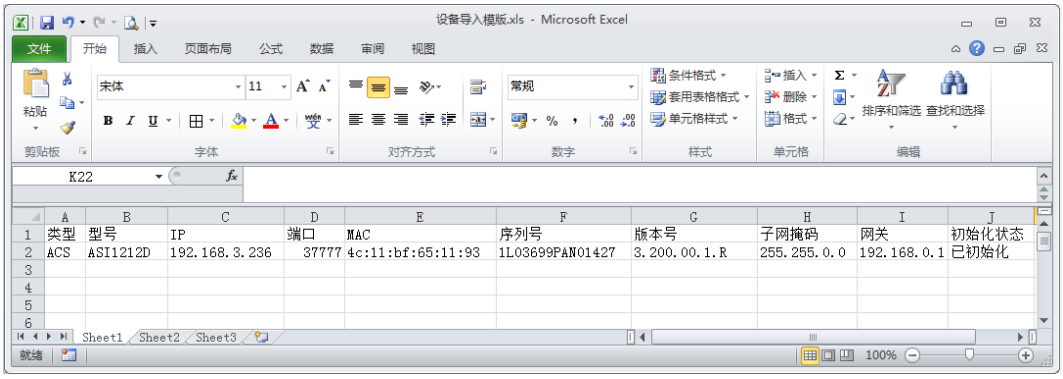
填写模板文件

步骤1　在工具的安装路径下获取并打开模板文件“设备导入模板.xls”，如图 2-3 所示。

说明

模板文件里提供的示例仅作参考，请根据实际情况填写。

图2-3 设备导入模板



步骤2　填写设备参数，具体参数说明请参见表 2-2。

表2-2 设备参数

参数	说明
类型	必选，设备的类型，填写 ACS。
型号	可选，设备的型号。
IP	必选，设备的 IP 地址。
端口	必选，设备的端口号。
MAC	必选，设备的 MAC 地址，请从设备标签上获取。
序列号	可选，设备的序列号。
版本号	可选，设备的版本号。
子网掩码	可选，设备的子网掩码。
网关	可选，设备的网关。
初始化状态	必选，包括“已初始化”和“未初始化”两种状态。

步骤3　保存并关闭模板文件。

导出设备信息文件

导出搜索到的设备信息，用于添加设备或者备份设备信息。

步骤1　单击。

系统显示“修改 IP”界面。

步骤2　选择需要导出的设备，并单击 导出。

系统弹出“另存为”对话框。

步骤3　选择保存路径，设置“文件名称”如“导出设备”。

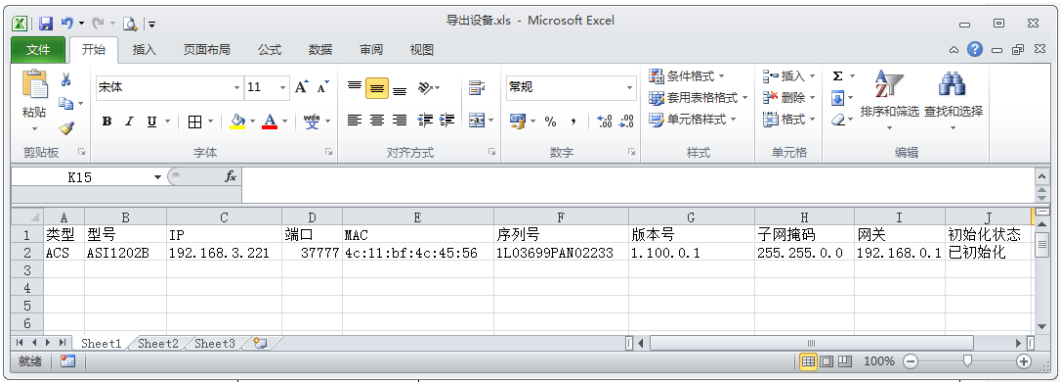
步骤4　单击“保存”，系统开始导出设备信息。

设备信息导出完成后，系统弹出提示对话框。

步骤5　单击“确定”。

可以在保存路径下查看导出的设备信息文件，如图 2-4 所示。

图2-4 导出设备信息



	A	B	C	D	E	F	G	H	I	J
1	类型	型号	IP	端口	MAC	序列号	版本号	子网掩码	网关	初始化状态
2	ACS	ASI1202B	192.168.3.221	37777	4c:11:bf:4c:45:56	1L03699PAN02233	1.100.0.1	255.255.0.0	192.168.0.1	已初始化
3										
4										
5										
6										

2.2.2.2 导入设备

获取模板后，通过在模板里添加设备信息并将模板导入系统来添加设备。

注意

使用模板文件导入设备时请先关闭模板文件。

步骤1　单击 。

系统显示“修改 IP”界面。

步骤2　单击 导入。

系统弹出“打开”界面。

步骤3　选择需要导入的设备文件，单击“打开”，系统开始导入设备。

设备导入完成后，系统弹出提示对话框。

步骤4　单击“确定”。

导入的设备显示在设备列表中，如图 2-5 所示。

图2-5 设备导入成功

2.3 初始化设备

单个或者批量初始化设备。

说明

- 部分设备支持此功能。
- 只能初始化局域网内的设备。
- 未初始化设备不能进行相关操作，在设备列表中显示为灰色，并且工具其他界面不提供未初始化设备的信息。

步骤1 单击 。

系统显示“修改 IP”界面。

步骤2 选择未初始化的设备。

步骤3 单击 初始化 。

系统显示“设备初始化”界面，如图 2-6 所示。

图2-6 设备初始化（1）

步骤4　选择需要初始化的设备，然后单击“初始化”。

系统显示“设备初始化”界面，如图 2-7 所示。

说明

- 不同型号设备的界面显示不同，请以实际为准。
- 若不设置预留信息，只能通过导 XML 文件重置密码。

图2-7 设备初始化（2）

步骤5　设置设备初始化参数，详细参数说明请参见表 2-3。

表2-3 设备参数说明

参数	说明
用户名	用户名默认为 admin。
新密码	输入设备的新密码。新密码设置规则包含以下两种，不同的设备支持不同的设置规则，请根据界面提示设置密码。 ● 设置为 8 位～32 位，可以由数字、字母和特殊字符（除“'”、“"”、“;”、“:”、“&”外）三种类型中的两种组成。 ● 只可设置为 4 位数字。
确认密码	确认输入的新密码。

参数	说明
预留手机	默认已选择，输入的手机号码将用于密码重置。

步骤6　单击“初始化”，系统开始初始化设备。

初始化完成后，系统显示如图 2-8 所示。

若初始化成功，显示✓；若初始化失败，显示⚠。单击图标可以查看详细信息。

图2-8 初始化完成

步骤7　单击“完成”，结束设备初始化操作。

初始化完成后，工具主界面上设备状态变为“已初始化”，设备信息将显示在工具其他界面。

2.4 修改 IP

单个或者批量修改设备的 IP 地址。

- 当设备较少或者设备的登录密码不相同时，可以单个修改设备的 IP 地址。
- 当设备较多且设备的登录密码相同时，可以批量修改设备的 IP 地址。

2.4.1 单个修改

当需要修改单个设备 IP 时，可选择此修改方式。

步骤1　单击IP。

系统显示“修改 IP”界面，如图 2-9 所示。

图2-9 修改 IP

步骤2　单击需要修改 IP 的设备对应的。

系统弹出“修改 IP”对话框，如图 2-10 所示。

说明

如果设备没在设备列表中，请重新搜索设备，详细操作请参见“2.2 添加设备”。

图2-10 修改 IP

步骤3　设置“模式”为“静态”，并填写设备的“目标 IP”、“子网掩码”和“网关”。

步骤4　单击“确定”，完成修改。

2.4.2 批量修改

当需要修改多个设备 IP 时，可选择此修改方式。

步骤1　单击。

系统显示“修改 IP”界面。

步骤2　选择需要修改 IP 的设备。

说明

如果设备没在设备列表中，请重新搜索设备，详细操作请参见“2.2 添加设备”。

步骤3　单击 批量修改IP 。

系统弹出“修改 IP”对话框，如图 2-11 所示。

图2-11 修改 IP

步骤4　设置“模式”为“静态”，并填写设备的“起始 IP”、“子网掩码”和“网关”。

说明

选择“同一 IP”，将选中的设备设置为同一个 IP 地址。

步骤5　单击“确定”，完成修改。

设备的 IP 地址从起始 IP 开始依次递增修改。

2.5 配置系统信息

可以校准设备时间、重启设备、恢复默认、修改密码和重置密码。

2.5.1 校准时间

通过设置校准设备的时间。

说明

目前设备不支持配置夏令时。

步骤1　单击 。

系统显示“系统配置”界面的“校时”页签，如图 2-12 所示。

图2-12 校时

步骤2　单击设备类型前的▶。

系统显示设备列表。

步骤3　选择单个或者多个设备。

说明

如果设备没在设备列表中，请重新搜索设备，详细操作请参见“2.2 添加设备”。

步骤4　根据实际情况选择设备同步时间的方式。

选择时间和时区，单击“手动同步”，设备时间同步为设置的时间。

单击“同步 PC”，以 PC 时间为基准调整设备时间。

选择“NTP 设置”，设置 NTP 服务器参数，参数说明请参见表 2-4。设置完成后单击“保存”。

表2-4 NTP 参数说明

参数	说明
NTP 服务器	设置为 NTP 服务器的 IP 地址或者域名。
NTP 端口	设置为对接 NTP 服务器的端口。
更新周期	设备向 NTP 服务器同步时间的间隔时间。

2.5.2 重启设备

手动重启设备。

注意

重启会造成业务中断，请尽量选择业务量小的时间重启设备。

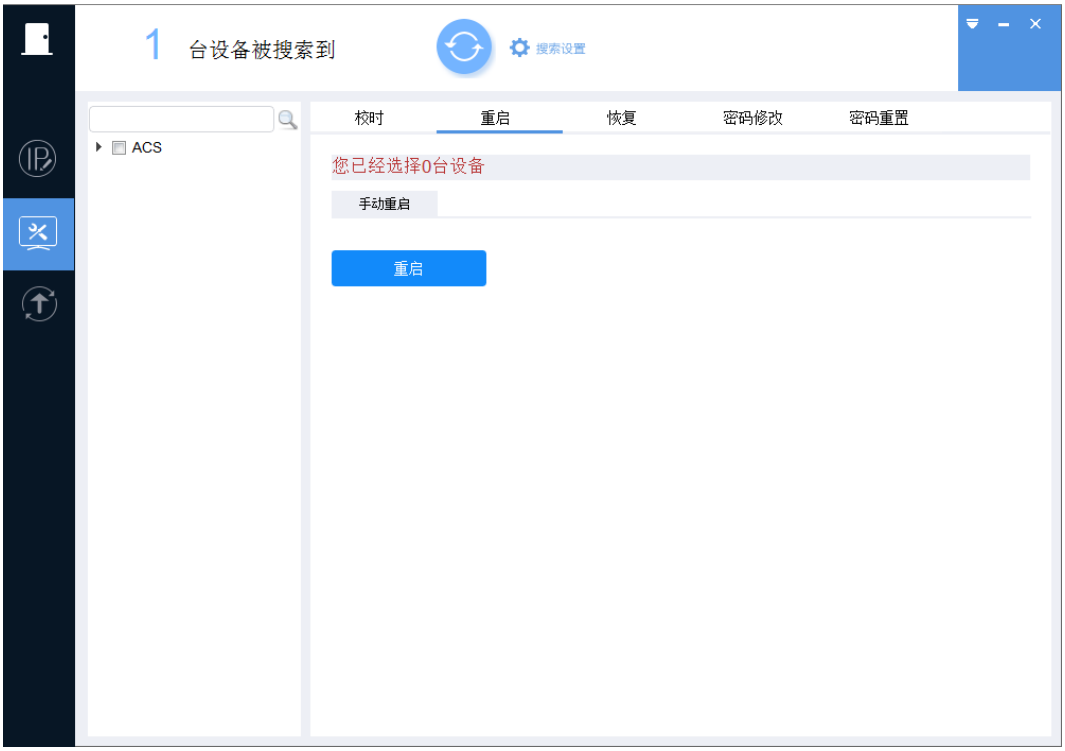
步骤1　单击。

系统显示“校时”界面。

步骤2　单击“重启”页签。

系统显示“重启”界面，如图 2-13 所示。

图2-13 重启



步骤3　单击设备类型前的 ▶ 。

系统显示设备列表。

步骤4　选择单个或者多个设备。

说明

如果设备没在设备列表中，请重新搜索设备，详细操作请参见“2.2 添加设备”。

步骤5　单击“重启”。

设备立即重启。

2.5.3 恢复默认

恢复设备的网络配置（不包括 IP 配置）、普通设置等。

说明

一体机、多门控制器恢复默认时，IP 也恢复为出厂默认 IP。

步骤1　单击 。

系统显示“校时”界面。

步骤2　单击“恢复”页签。

系统显示“恢复”界面，如图 2-14 所示。

图2-14 恢复

步骤3 单击设备类型前的▶。

系统显示设备列表。

步骤4 选择单个或者多个设备。

说明

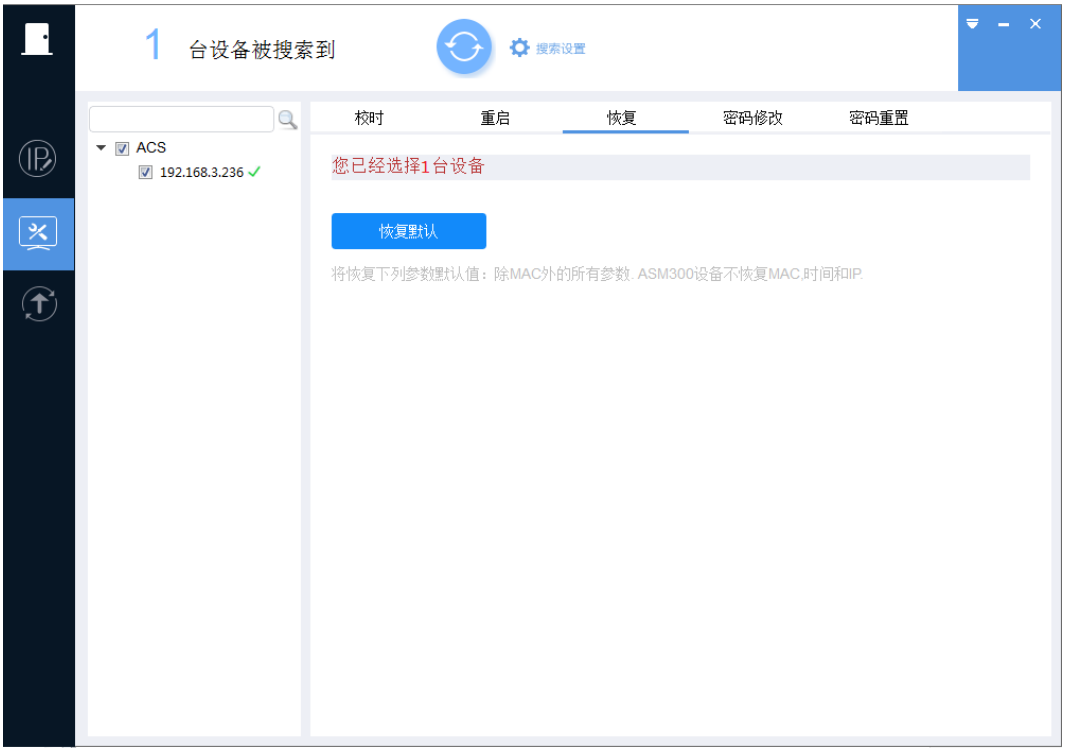
如果设备没在设备列表中，请重新搜索设备，详细操作请参见“2.2 添加设备”。

步骤5 单击“恢复默认”。系统开始恢复设备的默认设置。

恢复默认完成后，系统显示如图 2-15 所示界面。

若恢复默认成功，设备后面显示✓；若失败，显示⚠。单击图标可查看详细信息。

图2-15 设置结果



2.5.4 修改密码

修改设备的登录密码。

步骤1　单击 。

系统显示“校时”界面。

步骤2　单击“密码修改”页签。

系统显示“密码修改”界面，如图 2-16 所示。

图2-16 密码修改（1）

步骤3　单击设备类型前的 。

系统显示设备列表。

步骤4　选择单个或者多个设备。

说明

- 如果设备没在设备列表中，请重新搜索设备，详细操作请参见“2.2 添加设备”。
- 选择的多个设备的登录密码必须相同。

步骤5　输入设备旧密码，并单击“确定”。

系统显示“密码修改”界面，如图 2-17 所示。

图2-17 密码修改（2）

步骤6　输入设备的新密码和确认密码。

新密码设置规则包含以下两种，不同的设备支持不同的设置规则，请根据界面提示设置密码。

- 设置为 8 位～32 位，可以由数字、字母和特殊字符（除“'”、“"”、“;”、“:”、“&”外）三种类型中的两种组成。
- 只可设置为 4 位数字。

说明

设置新密码后，在使用“搜索设置”搜索设备时，请使用新密码登录设备。

步骤7　单击“确定”，完成修改密码。

说明

若新密码和旧密码重复，单击“确定”后，系统弹出提示对话框，单击“确定”并重新设置新密码。

2.5.5 重置密码

通过扫描二维码或者 XML 文件重置密码。

说明

- 只能对局域网内的设备进行密码重置。
- 若在初始化时没有设置预留信息，密码重置时只能通过 XML 文件方式。

2.5.5.1 二维码重置密码

通过扫描界面上的二维码重置密码，仅支持单个设备密码重置。

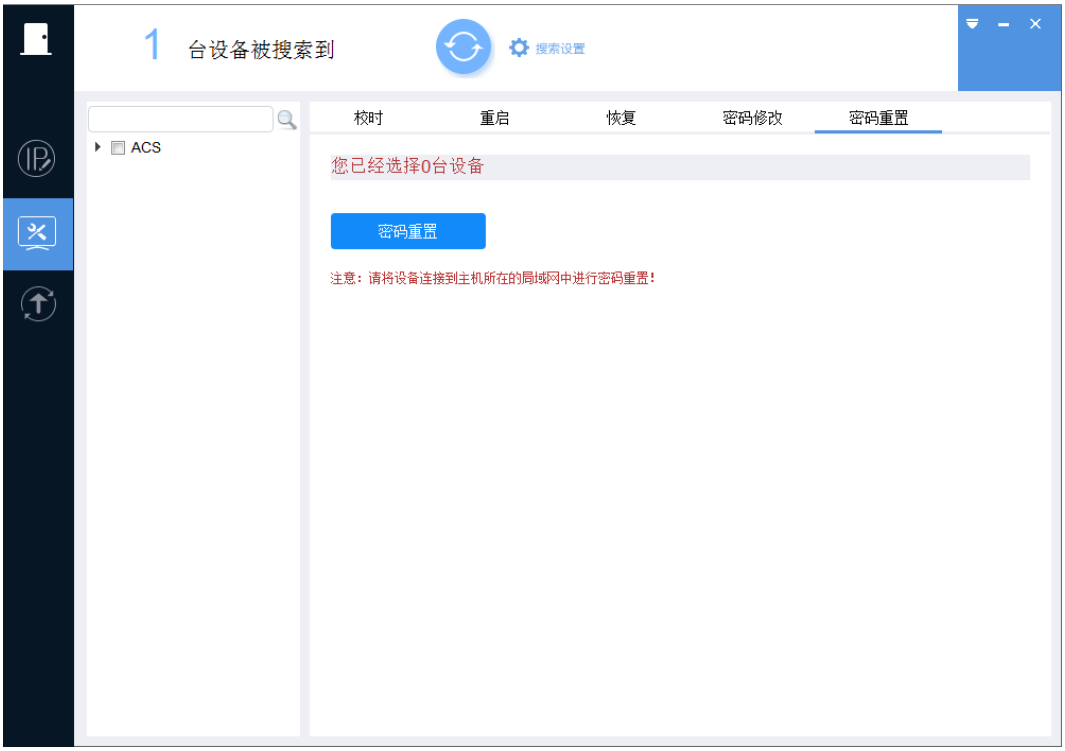
步骤1　单击。

系统显示“校时”界面。

步骤2　单击“密码重置”页签。

系统显示“密码重置”界面，如图 2-18 所示。

图2-18 密码重置



步骤3 单击设备类型前的 。

系统显示设备列表。

步骤4 选择需要重置密码的单个设备。

说明

如果设备没在设备列表中，请重新搜索设备，详细操作请参见“2.2 添加设备”。

步骤5 单击“密码重置”。

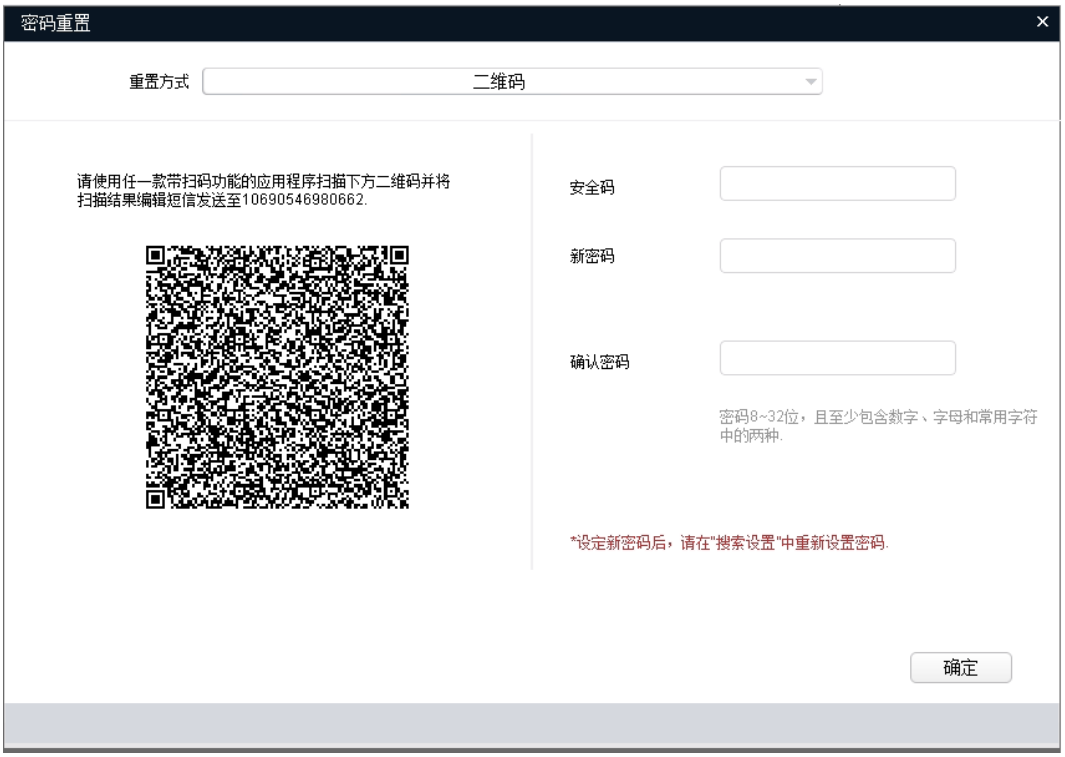
若设备不支持此功能，系统会显示提示信息。

若设备支持此功能，系统显示“密码重置”界面，如图 2-19 所示。

说明

不同型号设备的界面显示不同，请以实际为准。

图2-19 密码重置



步骤6　选择“重置方式”为“二维码”。

步骤7　根据实际界面指示操作，获取安全码。

注意

- 扫描二维码获取安全码时，一个二维码最多支持扫描获取两次安全码。
- 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。

步骤8　输入“安全码”、“新密码”和“确认密码”。

输入设备的新密码。新密码设置规则包含以下两种，不同的设备支持不同的设置规则，请根据界面提示设置密码。

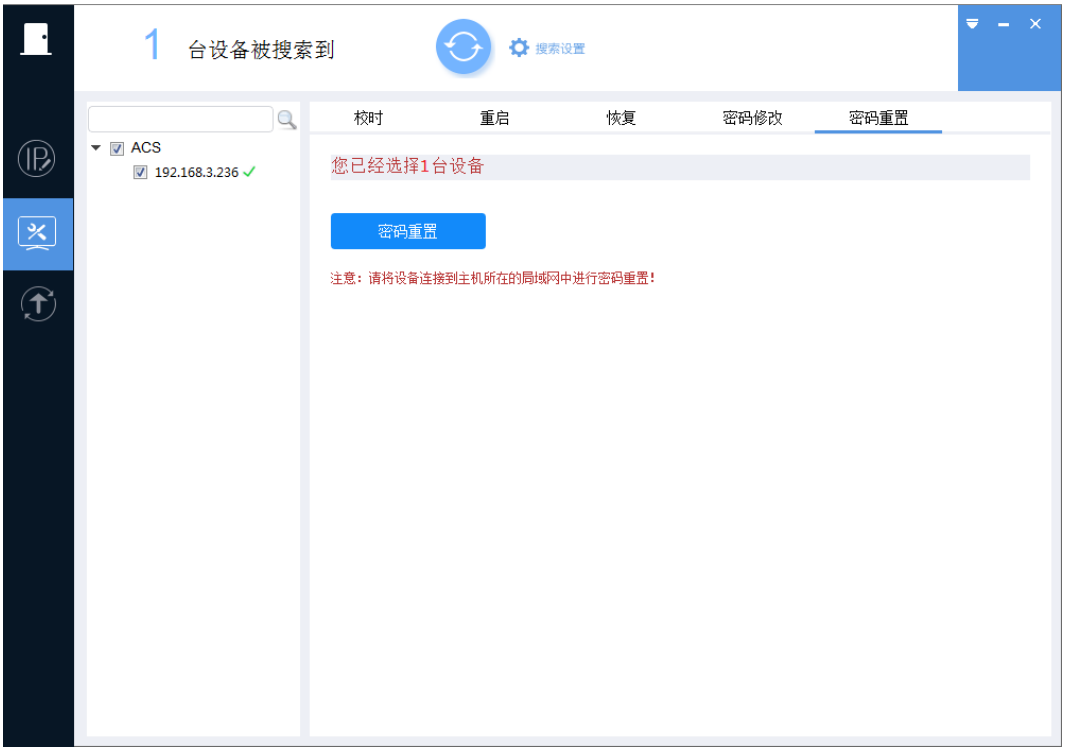
- 设置为 8 位～32 位，可以由数字、字母和特殊字符（除“'”、“"”、“;”、“:”、“&”外）三种类型中的两种组成。
- 只可设置为 4 位数字。

步骤9　单击“确定”，系统开始重置密码。

密码重置完成后，在设备处显示结果，如图 2-20 所示。

表示密码重置失败，表示密码重置成功。单击图标可以查看详细信息。

图2-20 密码重置结果



2.5.5.2 XML 文件重置密码

XML 支持单个或者多个设备密码重置。

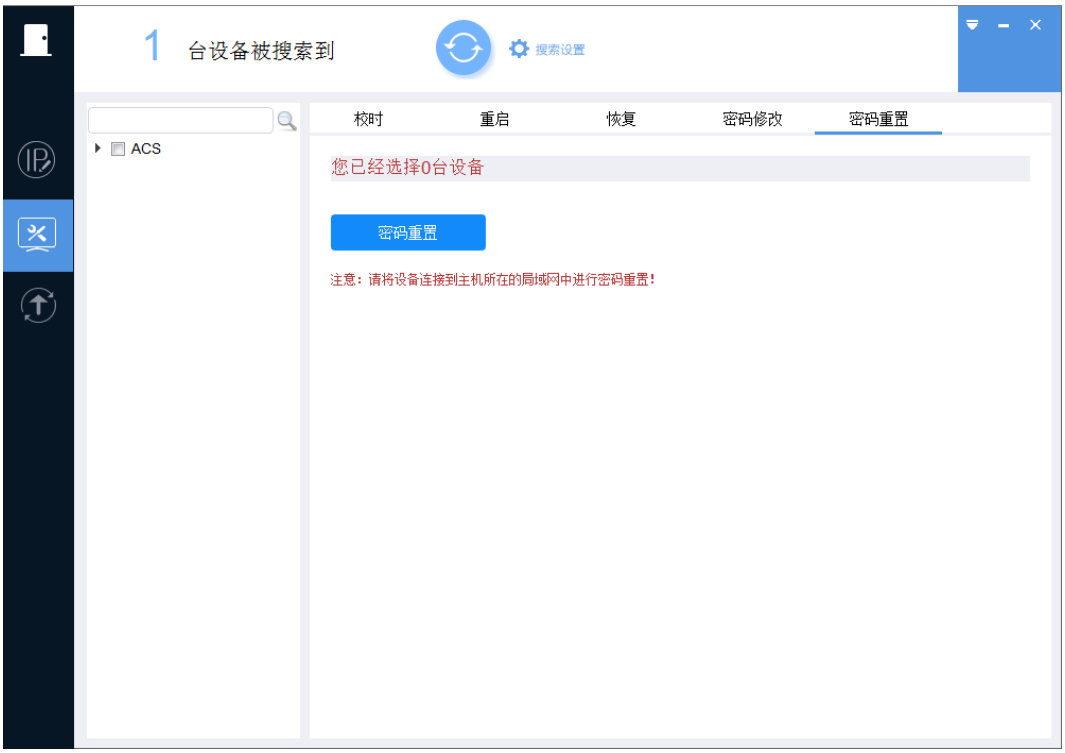
步骤1　单击 。

系统显示“校时”界面。

步骤2　单击“密码重置”页签。

系统显示“密码重置”界面，如图 2-21 所示。

图2-21 密码重置



步骤3　单击设备类型前的 。

系统显示设备列表。

步骤4　选择需要重置密码的单个或者多个设备。

说明

如果设备没在设备列表中，请重新搜索设备，详细操作请参见“2.2 添加设备”。

步骤5　单击“密码重置”。

若设备不支持此功能，系统会显示提示信息。

若设备支持此功能，系统显示“密码重置”界面，如图 2-22 所示。

说明

不同型号设备的界面显示不同，请以实际为准。

图2-22 密码重置

步骤6　选择“重置方式”为“XML 文件”。

系统显示“密码重置-导出 XML”界面，如图 2-23 所示。

说明

不同型号设备的界面显示不同，请以实际为准。

图2-23 密码重置-导出 XML

步骤7　导出 XML。

1. 单击“浏览”，选择导出 XML 文件的保存路径。
2. 单击“下一步”，开始导出。
   导出完成后，系统弹出提示对话框。
3. 单击“确定”，完成导出。
   导出 XML 文件成功后，系统自动进入“密码重置-导入 XML”界面。

步骤8 获取 result.xml 文件。

在 XML 文件的保存路径下找到 ExportFile.xml 文件，按照界面提示将此文件作为邮件附件发送至指定邮箱。约几分钟后，您会收到附件形式的 result.xml 文件，将其保存至任意路径。

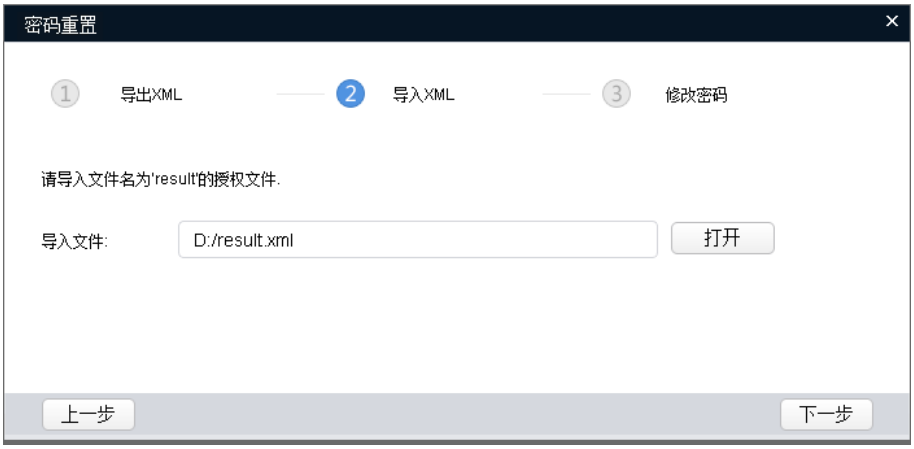
步骤9 导入 XML。

说明

若导入 XML 的窗口已关闭，可以选择“系统设置 > 密码重置”，单击“继续上次修改密码操作，请导入 XML 文件”，以继续操作。

1. 单击“打开”，从保存路径导入 result.xml 文件，如图 2-24 所示。

图2-24 密码重置-导入 XML



2. 单击“下一步”，开始导入。
   导入 XML 文件成功后，系统自动进入“密码重置-修改密码”界面，如图 2-25 所示。

图2-25 密码重置-修改密码

步骤10 修改密码。

输入设备的新密码。新密码设置规则包含以下两种，不同的设备支持不同的设置规则，请根据界面提示设置密码。

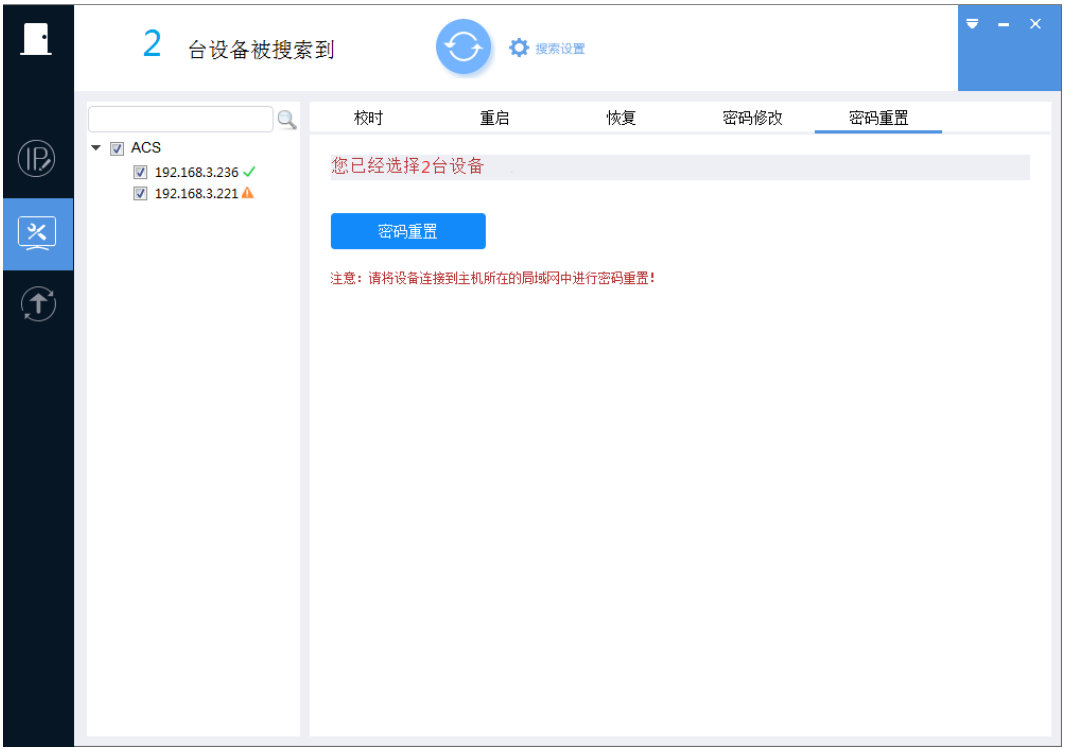
- 设置为 8 位～32 位，可以由数字、字母和特殊字符（除“'”、“"”、“;”、“:”、“&”外）三种类型中的两种组成。
- 只可设置为 4 位数字。

步骤11 单击“完成”，系统开始重置密码。

密码重置完成后，在设备处显示结果，如图 2-26 所示界面。

表示有参数配置失败，表示参数均配置成功。单击图标可以查看详细信息。

图2-26 设置结果



2.6 升级设备

单个或者批量升级设备。

说明

升级过程中如果设备断连，只要 ACSConfig 继续停留在升级界面，当设备再次连上网络，会继续上次的升级。

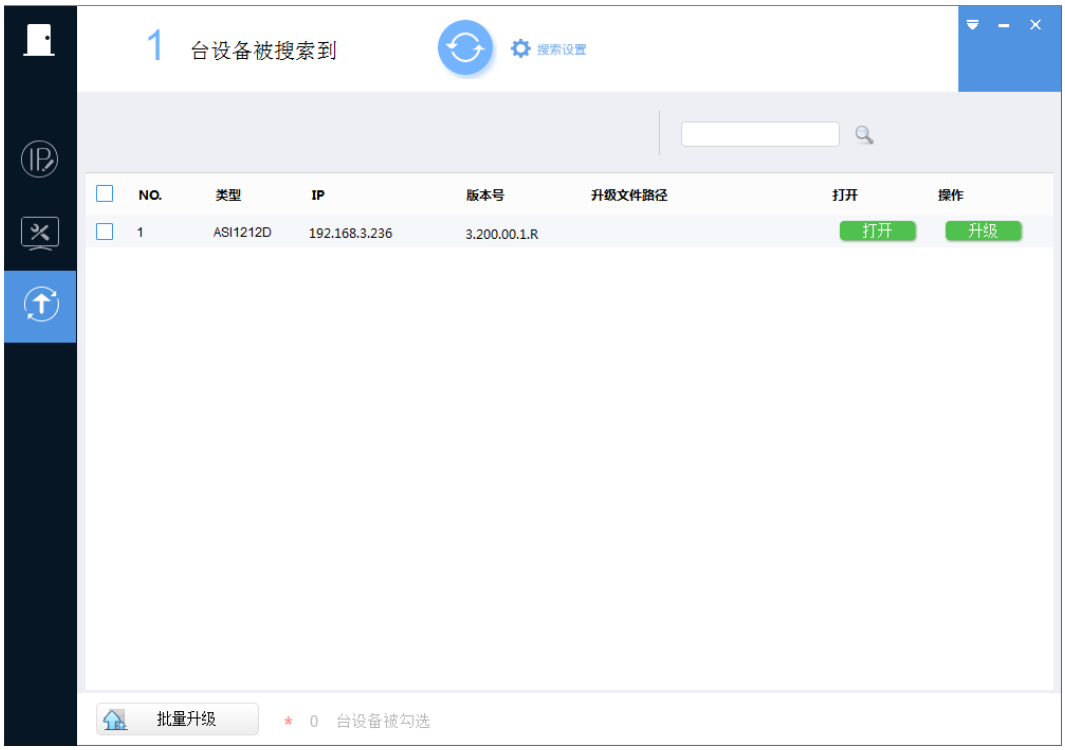
2.6.1 单个升级

当需要升级单个设备时，可选择此升级方式。

步骤1　单击。

系统显示“升级”界面，如图 2-27 所示。

图2-27 升级



步骤2 单击需要升级设备对应的“打开”，选择升级文件，并单击“打开”。

说明

如果设备没在设备列表中，请重新搜索设备，详细操作请参见“2.2 添加设备”。

步骤3 单击“升级”，系统开始升级并显示进度。

升级完成后，设备自动重新启动。

2.6.2 批量升级

将多个设备批量升级到同一软件版本。

步骤1 单击 。

系统显示“升级”界面。

步骤2 选择需要升级设备。

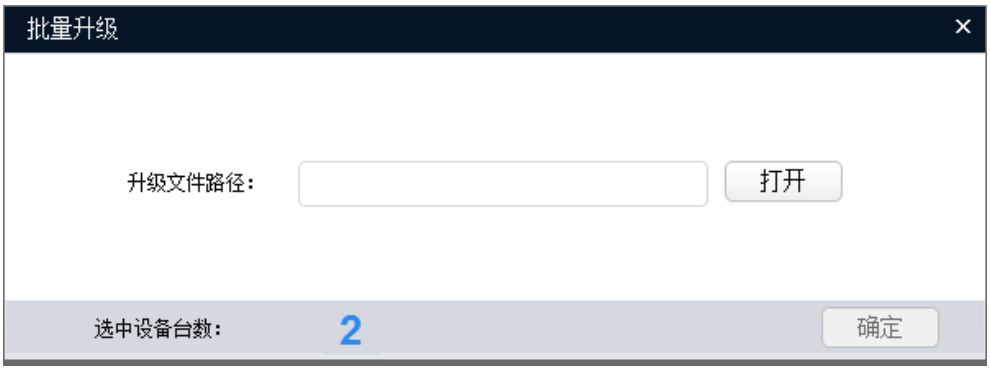
说明

- 如果设备没在设备列表中，请重新搜索设备，详细操作请参见“2.2 添加设备”。
- 选择的设备必须是升级到同一个软件版本的设备。

步骤3 单击 批量升级 。

系统弹出“批量升级”对话框，如图 2-28 所示。

图2-28 批量升级



步骤4　单击“打开”，选择升级文件。

步骤5　单击“确定”，系统开始升级。