



设备初始化及密码重置

说明书

V1.0.0

浙江大华技术股份有限公司

版权声明

© 2017 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。

关于本文档

- 产品请以实物为准，本文档仅供参考。
- 本文档供多个型号产品做参考，每个产品的具体操作不一一例举，请用户根据实际产品自行对照操作。

- 如不按照本文档中的指导进行操作，因此而造成的任何损失由使用方自己承担。
- 如获取到的 PDF 文档无法打开，请将阅读工具升级到最新版本或使用其他主流阅读工具。
- 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。产品部分功能在更新前后可能存在细微差异。
- 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。

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. 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。请访问大华官网获取最新版本的固件。

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的。

9. 限制普通账户的权限

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经授权的用户没有机会访问到这些设备。

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。

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上，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 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。

概述








为增强大华设备的安全性，确保对用户信息的保护，大华产品新增设备初始化及密码重置功能。用户首次登录设备时需要设置用户名和密码。用户忘记密码时，可通过扫描二维码或回答密保问题（密保问题方式仅支持在本地输出界面上使用）找回密码。

适用型号

本文档适用于大华通用产品，为帮助用户更好地理解大华网络产品的设备初始化与密码重置特性。

符号约定

在本文中可能出现下列标志，代表的含义如下。

符号	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。
 电击防护	表示高压危险。
 激光防护	表示强激光辐射。
 防静电	表示静电敏感的设备。
 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	2017.11.7

法律声明	I
网络安全声明和建议	III
使用安全须知	V
前言	VI
1 概述	1
2 设备初始化	2
2.1 设备初始化	2
2.2 ConfigTool 工具初始化	4
2.3 SmartPSS 平台初始化	8
3 密码重置	10
3.1 WEB 界面重置	10
3.2 ConfigTool 工具重置	12
3.3 SmartPSS 平台重置	14

1 概述

为持续完善大华产品的安全性能和响应国家网络信息安全的要求，大华对现有网络设备的密码策略进行调整，增加“首次开机初始化”、“密码重置”功能。意在提升用户的信息安全意识，规避默认密码或弱密码带来的安全风险。

首次开机初始化： 取消现有的默认密码方案，设备首次开机和恢复出厂设置时强制用户设定 admin 账户密码，密码需为 8-32 位，且至少包含数字、字母和常用字符中的两种或两种以上类型组合，才能进行密码初始化操作。

目前可采用 Web 界面、Configtool、NVR/DVR 还可通过本地界面初始化。

密码重置： 用户忘记密码后，可通过以下两种方式重设密码（仅适用于 admin 账户），具体操作步骤参考附件：

- 1) **扫描二维码：** 在初始化过程的配置界面，用户可设置 admin 账户的手机号码。忘记密码后，通过扫描二维码接收服务运营商发送的安全码，验证通过后即可重置密码。
- 2) **安全问题：** 回答预先设置的安全问题，验证通过后可重置密码。该方式仅 NVR/DVR 的本地界面支持。

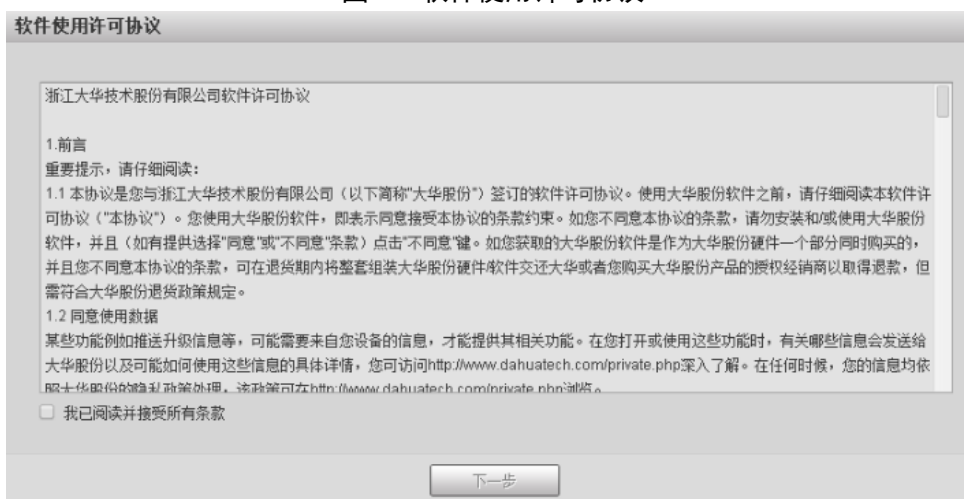
10 月起生产的网络设备产品全面支持密码初始化和密码重置功能（NVR 前期已支持），对于密码政策调整可能给您带来的不便，敬请谅解！

参数	说明
预留手机	<p>设置预留手机号码用于密码重置，默认已选择。</p> <p>扫描二维码重置密码时，需要使用预留手机接收安全码，通过安全码重置 admin 用户的密码。</p> <p>如果未设置预留手机号码或者需要变更预留手机号码，您可以选择“设置 > 系统管理 > 用户管理 > 用户管理 > 用户”界面进行设置。</p>

步骤3 单击“确定”。

系统显示“软件使用许可协议”界面，如图 2-2 所示。

图2-2 软件使用许可协议



步骤4 选择“我已阅读并接受所有条款”，单击“下一步”。

系统显示“云接入”界面，如图 2-3 所示。

图2-3 云接入



步骤5 根据实际需要选择“云接入”，实现设备的乐橙云注册，单击“下一步”。

系统显示“在线升级”界面，如图 2-4 所示。

图2-4 在线升级



步骤6 根据实际需要设置升级方式。

选择“自动检测”，有系统更新时自动提示，系统每1天自动检查一次。

 说明


登录后，您也可以在“设置 > 系统管理 > 系统升级 > 在线升级”中设置。

步骤7 单击“确定”。

设备初始化完成。

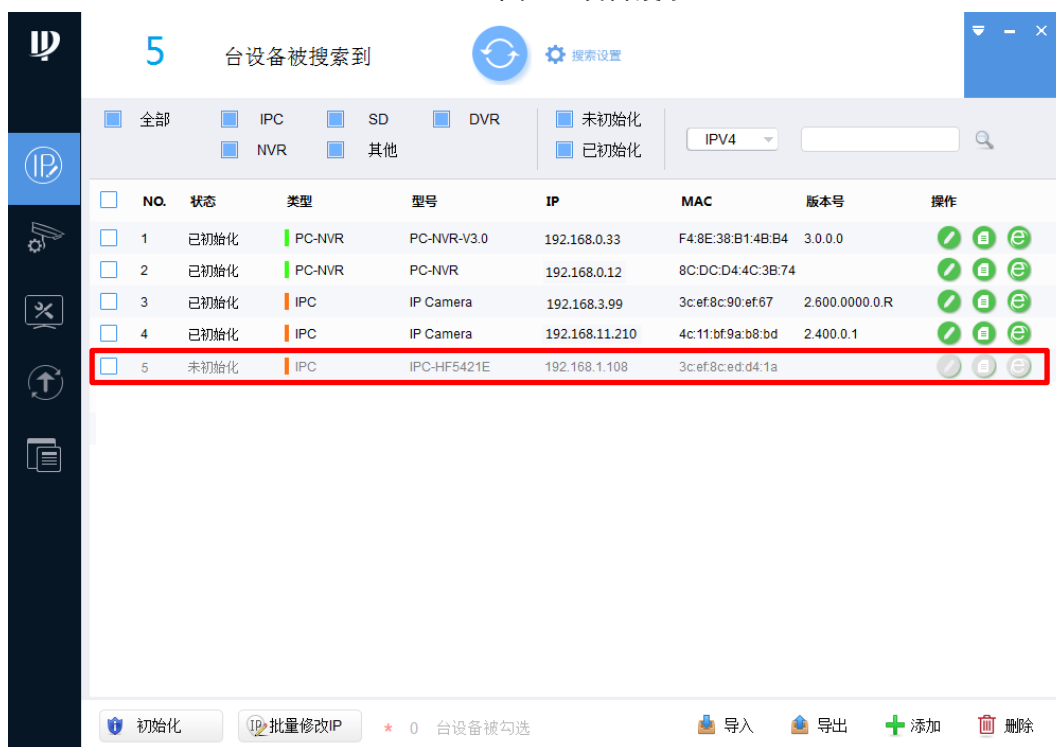
2.2 ConfigTool 工具初始化

操作步骤：

步骤1 双击桌面上的快捷键 ，系统将进入主界面(4.07 及以上版本支持)。

步骤2 单击  进入“修改 IP”界面。

图2-5 设备搜索



步骤 3 选择未初始化的设备，单击 初始化。系统显示“设备初始化”界面。

图2-6 选择未初始化设备



步骤 4 选择需要初始化的设备，单击“初始化”。

图2-7 设备初始化

1 台设备未初始化

用户名

新密码

弱 中 强

确认密码

密码8~32位, 且至少包含数字、字母和常用字符中的两种.

预留手机 (用于密码重置)

*设定新密码后, 请在“搜索设置”中重新设置密码.

初始化

说明

不同型号设备的界面显示不同, 请以实际为准。

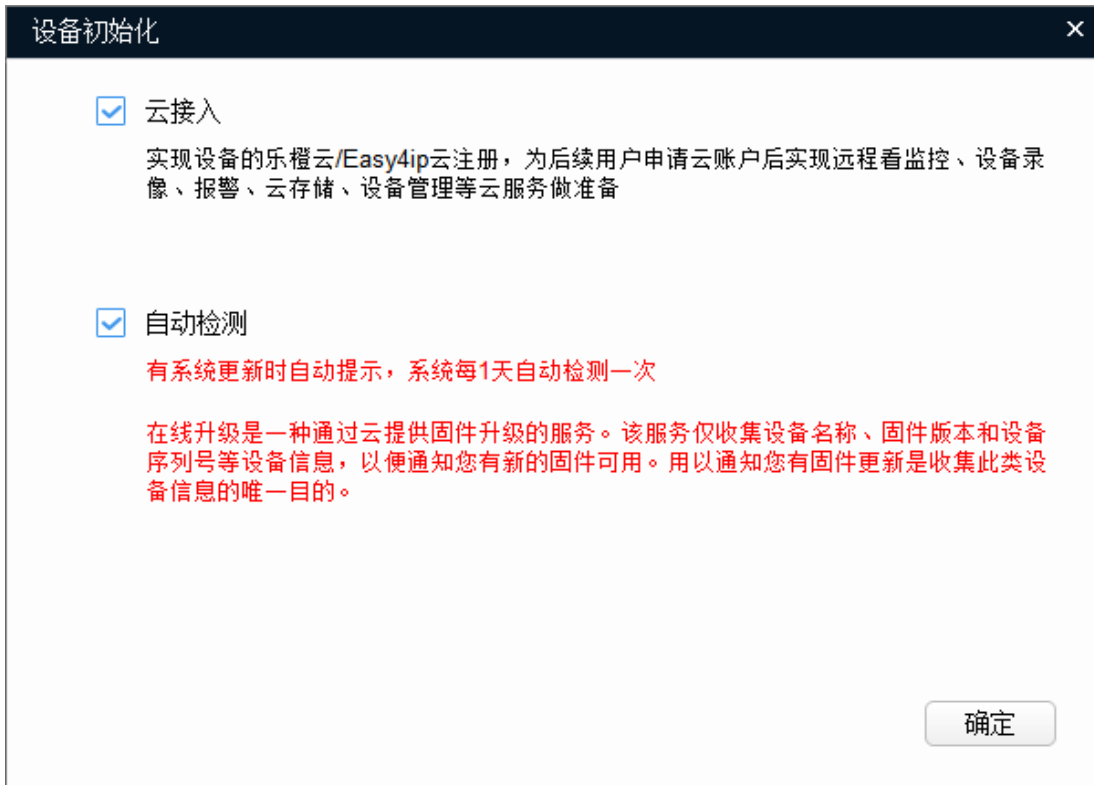
步骤 5 设置设备初始化参数, 详细参数说明请参见下表。

表2-2 设备初始化参数

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。请根据密码强弱提示设置高安全性密码。 新密码可设置为 8 位~32 位, 必须由数字、字母和特殊字符 (除 “'”、“”、“;”、“:”、“&” 外) 三种类型中的至少两种组成。
确认密码	确认输入的新密码。
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”, 系统显示“设备初始化”界面。

图2-8 设备初始化云接入或自动检测



步骤 7 根据您的实际需求为设备选择“云接入”和“自动检测”功能。

步骤 8 单击“确定”，系统开始初始化设备。初始化完成后，系统显示如下图所示界面。

- 若初始化成功，显示✔。
- 若初始化失败，显示⚠。

图2-9 初始化完成



步骤 9 单击“完成”，结束设备初始化操作。初始化完成后，ConfigTool 主界面上设备状态变为“已初始化”，设备信息将显示在其他界面。

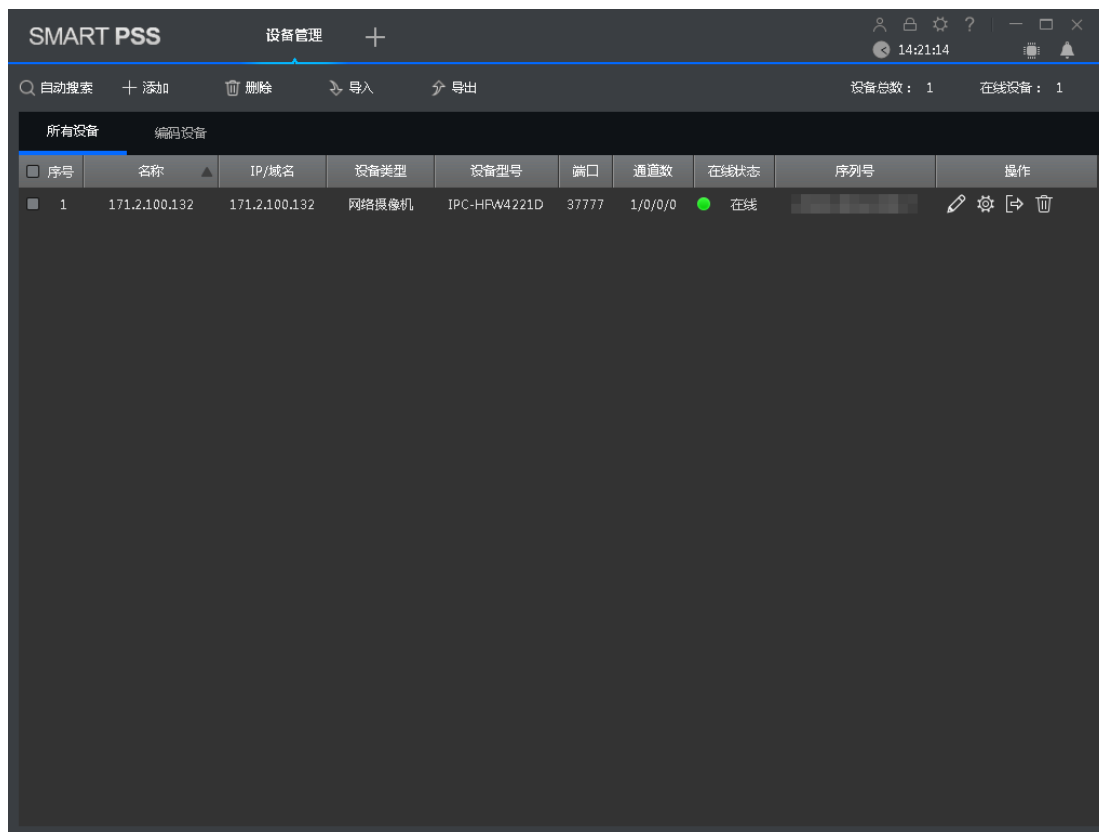
2.3 SmartPSS 平台初始化

操作步骤:

步骤 1 打开并登录 SmartPSS 客户端。

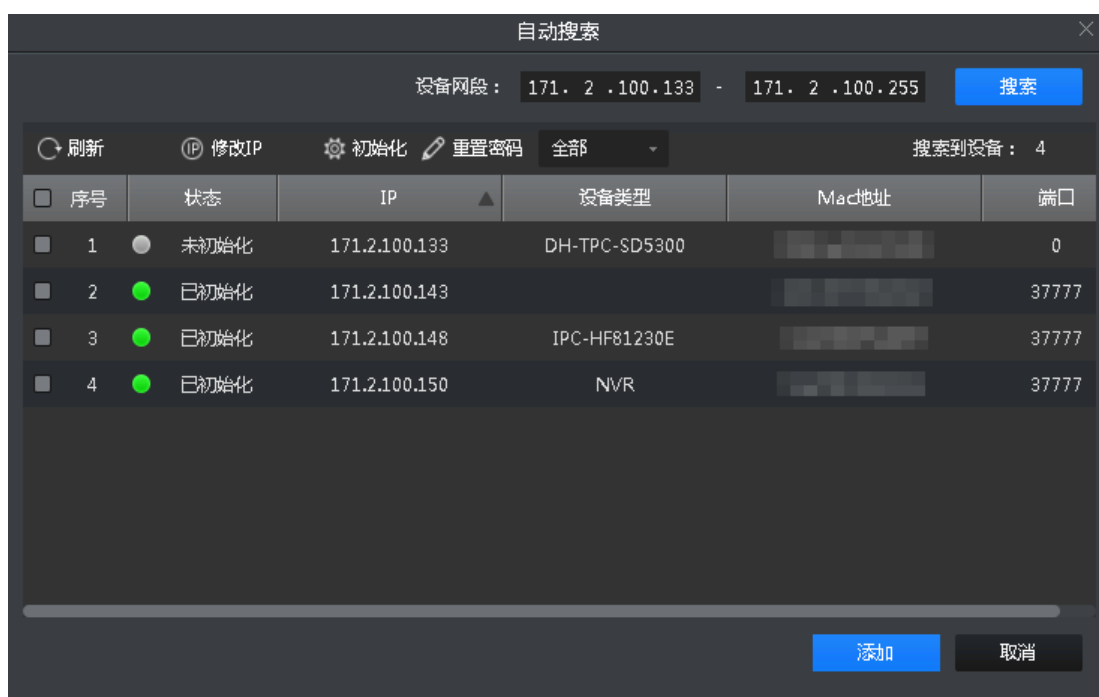
步骤 2 在“新功能”界面，单击“设备管理”。

图2-10 设备管理



步骤 3 单击“自动搜索”。

图2-11 自动搜索



步骤 4 选择未初始化的设备，单击“初始化”。

图2-12 初始化设备

初始化设备

1台设备初始化

用户名 admin

密码

密码强度

确认密码

绑定电话 (重置设备密码)

电话号码

此信息用于密码找回，请不要随意填写！NVS, NVD, M60等设备不需要设置！

初始化

步骤 5 设置 admin 用户的密码和预留手机。

步骤 6 单击“初始化”。系统显示设备初始化进度，初始化完成后如图所示。

图2-13 初始化完成

初始化设备

1台设备初始化


初始化设备完成!

100%

序号	序列号	IP	MAC	结果
1		192.168.1.108		成功

3 密码重置

当您忘记 admin 用户的密码时，可以通过密码重置功能，自助设置新的密码。密码重置支持通过扫描二维码方式。

 说明

密码重置仅支持 admin 用户。

3.1 WEB 界面重置

当您忘记了 admin 用户的密码时，可以通过预留手机重置密码。

步骤1 打开 IE 浏览器，在地址栏输入摄像机的 IP 地址，按【Enter】键。

连接成功后，系统显示“登录”界面，如图 3-1 所示。

图3-1 登录



步骤2 单击“忘记密码?”。

系统显示“密码重置”界面，如图 3-2 所示。

图3-2 密码重置 (1)



步骤3 重置登录密码。

根据界面提示扫描实际界面的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。



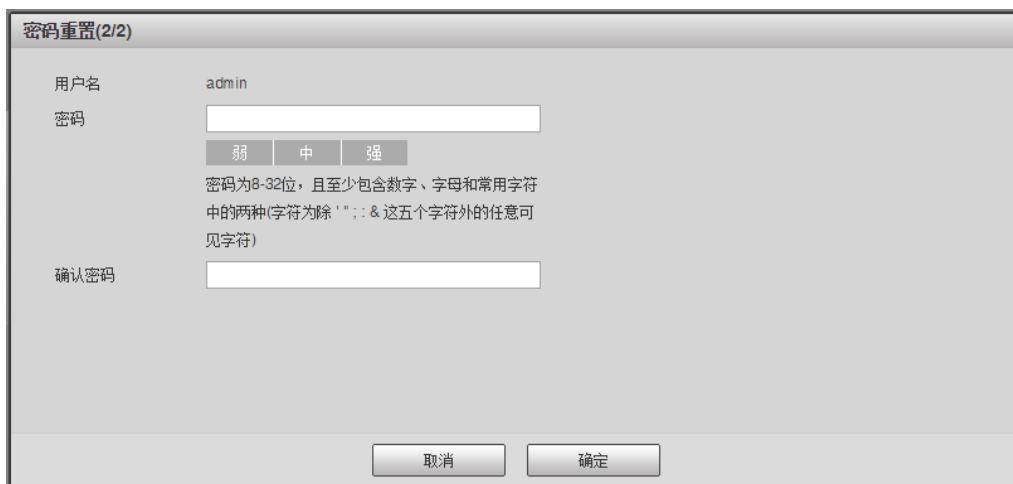
注意

- 推荐使用大华售后微信和大华售后 APP 直接扫描界面二维码。
- 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。
- 若连续两次获取安全码未使用，则第三次获取安全码系统会提示失败。如需正常使用设备，需硬件恢复设备默认设置后重新初始化设备设置新密码后开始使用设备，或者等到 24 小时之后重新获取。
- 预留手机号码填写错误的情况，请联系客服热线处理。
- 若在忘记密码之前没有预留过手机号码，则 Web 端不支持进行密码重置，需要咨询经销商或当地技术支持协助。

步骤4 单击“下一步”。

系统显示设置新密码界面，如图 3-3 所示。

图3-3 重置密码 (2)



- 步骤5 重新设置“密码”和“确认密码”。
密码可设置为 8 位~32 位非空字符，必须由数字、字母和常用字符（除“'”、“”、“;”、“:”、“&”外）三种类型中的至少两种组成。请根据密码强弱提示设置高安全性密码。
- 步骤6 单击“确定”，完成密码重置。
系统显示“登录”界面。

3.2 ConfigTool 工具重置

支持扫描二维码重置密码。仅支持重置同一局域网内的前端设备密码。
通过扫描界面上的二维码重置密码，一次只支持一台设备密码重置。



- 步骤1 双击桌面上的快捷图标。
系统显示主界面。
- 步骤2 单击。
系统显示系统设置界面。
- 步骤3 单击“密码重置”页签。
系统显示“密码重置”界面，如图 3-4 所示。

图3-4 密码重置



- 步骤4 单击设备类型前的▾，选择需要重置密码的设备。
- 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 3-5 所示。

说明

不同型号设备的界面显示不同，请以实际为准。

图3-5 密码重置



步骤6 选择“重置方式”为“二维码”。

步骤7 根据界面提示扫描二维码，并获取安全码。

步骤8 输入“安全码”、“新密码”和“确认密码”。

密码可设置为 8 位~32 位非空字符，可以由大写字母、小写字母、数字和特殊字符（除“!”、“”、“;”、“:”、“&”外）组成，且至少包含 2 类字符。新密码和确认密码保持一致。请根据密码强弱提示设置高安全性密码。

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 3-6 或者图 3-7 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3-6 密码重置结果（1）



图3-7 密码重置结果 (2)



3.3 SmartPSS 平台重置

支持扫描二维码重置密码。仅支持重置同一局域网内的前端设备密码。

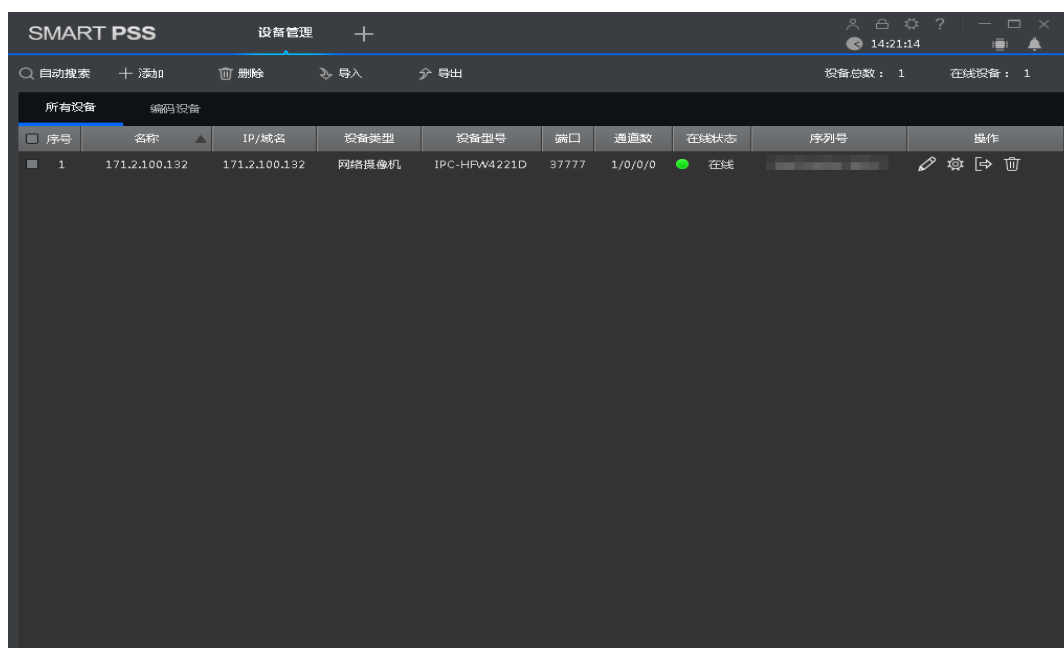
通过扫描界面上的二维码重置密码，一次只支持一台设备密码重置。

步骤1 打开并登录 SmartPSS 客户端。

步骤2 在“新功能”界面，单击“设备管理”。

系统显示“设备管理”界面，如图 3-8 所示。

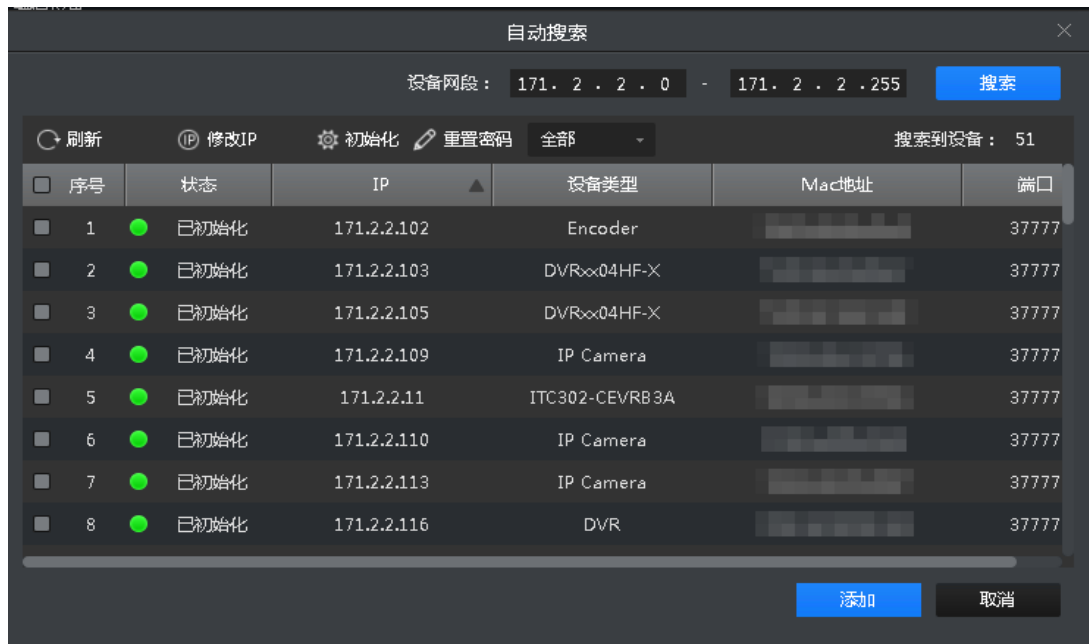
图3-8 设备管理



步骤3 单击“自动搜索”。

系统显示“自动搜索”界面，如图 3-9 所示。

图3-9 自动搜索



步骤4 选择一台需要重置密码的设备，单击“重置密码”。

系统显示“重置密码”界面，如图 3-10 所示。

图3-10 重置密码 (1)



步骤5 根据界面提示扫描二维码，并获取安全码。

步骤6 在“请输入安全码”文本框中输入接收到的安全码，单击“下一步”。

系统显示设置新密码界面，如图 3-11 所示。

图3-11 重置密码 (2)



重置密码

用户名 admin

密码

密码强度

确认密码

密码重置 取消

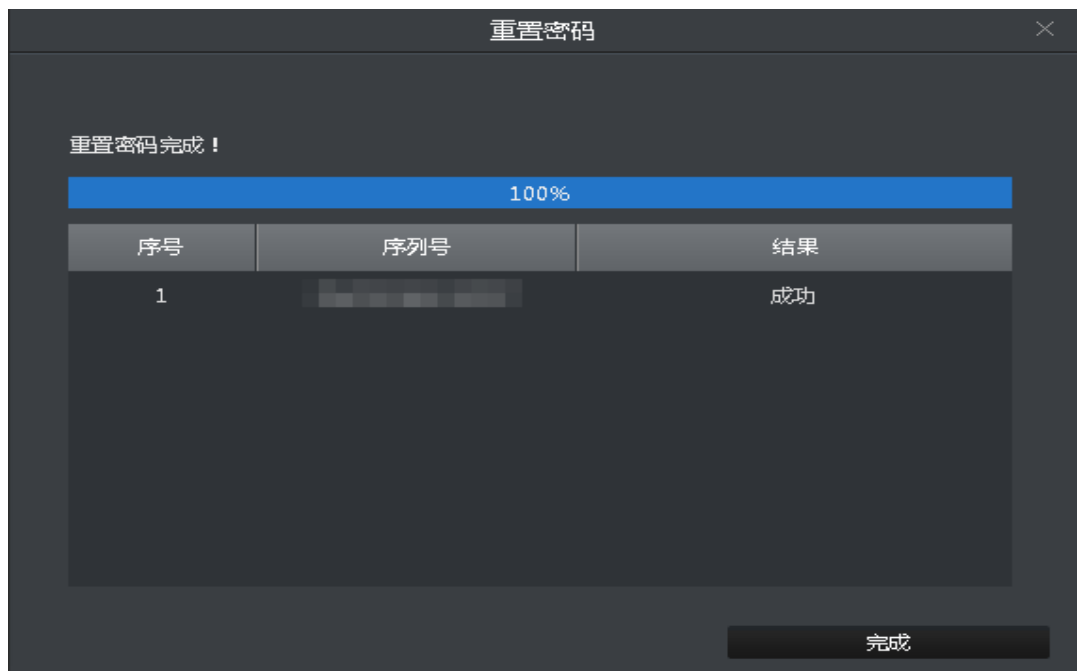
步骤7 输入“密码”和“确认密码”。

密码可设置为 8 位~32 位非空字符，可以由大写字母、小写字母、数字和特殊字符（除“'”、“””、“;”、“:”、“&”外）组成，且至少包含 2 类字符。新密码和确认密码保持一致。请根据密码强弱提示设置高安全性密码。

步骤8 单击“密码重置”。

系统显示密码重置进度，密码重置完成后如图 3-12 所示。

图3-12 重置密码 (3)



重置密码

重置密码完成!

100%

序号	序列号	结果
1		成功

完成

步骤9 单击“完成”，完成密码重置。

【社会的安全 我们的责任】

SOCIAL SECURITY IS OUR RESPONSIBILITY



浙江大华技术股份有限公司

地址：杭州市滨江区滨安路1187号

邮政编码：310053

客服热线：400-672-8166

公司网址：www.dahuatech.com