



(12) 发明专利

(10) 授权公告号 CN 110073335 B

(45) 授权公告日 2023. 07. 28

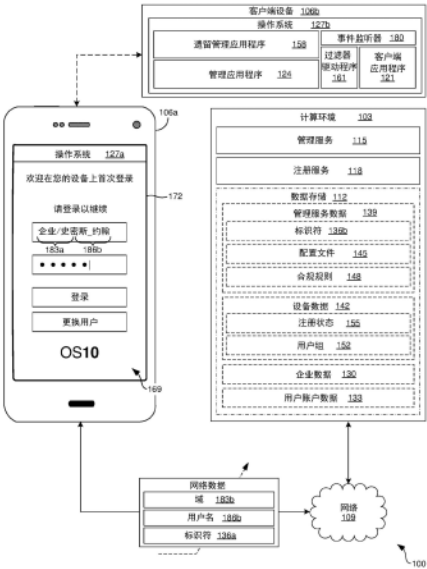
(21) 申请号 201780076252.4	(72) 发明人 J·罗斯扎克 V·默西
(22) 申请日 2017.12.07	S·尚萨拉姆 B·瓦特
(65) 同一申请的已公布的文献号	K·雷古拉
申请公布号 CN 110073335 A	(74) 专利代理机构 北京市磐华律师事务所
(43) 申请公布日 2019.07.30	11336
(30) 优先权数据	专利代理师 高伟 姜晓丹
15/373,603 2016.12.09 US	(51) Int.Cl.
(85) PCT国际申请进入国家阶段日	G06F 9/48 (2006.01)
2019.06.10	(56) 对比文件
(86) PCT国际申请的申请数据	US 2011/093953 A1,2011.04.21
PCT/US2017/065181 2017.12.07	CN 103503364 A,2014.01.08
(87) PCT国际申请的公布数据	US 2014/0331297 A1,2014.11.06
W02018/106962 EN 2018.06.14	审查员 殷娉
(73) 专利权人 威睿公司	
地址 美国加利福尼亚州	权利要求书1页 说明书13页 附图6页

(54) 发明名称

管理应用程序的共存和多个用户设备管理

(57) 摘要

提供了用于提供在客户端设备上执行第一管理应用程序和第二管理应用程序两者的各种示例。在一个示例中,客户端设备可以配置为识别安装在客户端设备上的第一管理应用程序(例如,遗留管理应用程序)对客户端设备的操作系统具有管理权限。由于第一管理应用程序配置为响应于检测到第二管理应用程序而生成终止命令,因此可以在操作系统接收到终止命令之前拦截终止命令。因此,操作系统不终止客户端设备上第二管理应用程序的执行,从而允许第一管理应用程序和第二管理应用程序在客户端设备上共存。



1. 一种用于提供第一管理应用程序和第二管理应用程序两者在客户端设备上的执行的方法,所述方法包括:

识别安装在所述客户端设备上的所述第一管理应用程序通过将所述客户端设备注册到第一远程服务而对所述客户端设备的操作系统具有设备管理权限;

在所述客户端设备上安装所述第二管理应用程序,所述第二管理应用程序被配置为通过将所述客户端设备注册到第二远程服务而获得对所述客户端设备的所述操作系统的设备管理权限;

在所述操作系统接收到由所述第一管理应用程序生成以终止执行任何其他管理应用程序的终止命令之前拦截所述终止命令,终止执行任何其他管理应用程序包括终止执行所述第二管理应用程序,由此所述操作系统不终止执行所述客户端设备上的所述第二管理应用程序;以及

响应于所述终止命令被拦截,使所述客户端设备向所述第一管理应用程序传送欺骗响应,就好像所述终止命令已经被所述操作系统接收到一样。

2. 根据权利要求1所述的方法,其中拦截所述终止命令由所述第二管理应用程序执行。

3. 根据权利要求1所述的方法,其中拦截所述终止命令由休眠代理应用程序执行。

4. 根据权利要求1所述的方法,进一步包括:使得所述客户端设备通过所述客户端设备的所述操作系统安装过滤器驱动程序,其监控至少一个预定义的应用程序编程接口API调用。

5. 根据权利要求4所述的方法,其中拦截所述终止命令是由所述过滤器驱动程序响应于检测到所述至少一个预定义的API调用而执行的。

6. 根据权利要求1所述的方法,进一步包括:使得所述客户端设备卸载所述客户端设备上的所述第一管理应用程序。

7. 根据权利要求1所述的方法,其中所述终止命令由所述第一管理应用程序定期生成,或者响应于检测到所述第二管理应用程序而生成。

8. 一种计算机可读介质,具有程序代码,所述程序代码在被执行时,使得客户端设备执行权利要求1-7中任一项所述的方法。

9. 一种提供第一管理应用程序和第二管理应用程序两者在客户端设备上的执行的系统,包括:

包括硬件处理器的所述客户端设备;以及

在所述客户端设备中可执行的程序指令,当其被所述客户端设备执行时,使得所述客户端设备执行权利要求1-7中任一项所述的方法。

管理应用程序的共存和多个用户设备管理

[0001] J·罗斯扎克;V·默西;S·尚萨拉姆;B·瓦特;K·雷古拉

[0002] 相关申请的交叉引用

[0003] 本申请要求于2016年12月9日提交的序列号为15/373,603的美国专利申请的权益,其全部内容通过引用并入本文中。

技术领域

[0004] 本申请涉及管理应用程序的共存和多个用户设备管理。

背景技术

[0005] 随着在工作场所自携设备(BYOD)技术的出现,企业允许员工或其他人员将自己的设备用于商业目的。这可以包括访问企业数据,如电子邮件和公司文档。但是,在员工在工作场所使用自己的设备之前,企业可以要求员工注册到管理服务,该管理服务能够保护通过设备可访问的企业数据免遭盗窃、数据丢失和未经授权的访问。管理服务的管理员可以使用管理服务来监督注册到服务或由服务管理的设备的操作。

[0006] 各种操作系统不允许或提供在单个设备上存在多个管理应用程序的能力。例如,系统中心配置管理器(SCCM)是由Microsoft®提供的设备管理应用程序,其能够评估、部署和更新企业环境中的设备。但是,在安装在设备上时,SCCM会更新设备的注册表,以防止其他管理应用程序执行管理功能。例如,SCCM可以对设备的操作系统进行应用程序编程接口(API)调用,以终止在设备上执行的任何其他管理服务。

发明内容

[0007] 本发明涉及一种用于提供第一管理应用程序和第二管理应用程序两者在客户端设备上的执行的方法,所述方法包括:识别安装在所述客户端设备上的所述第一管理应用程序通过将所述客户端设备注册到第一远程服务而对所述客户端设备的操作系统具有设备管理权限;在所述操作系统接收到由所述第一管理应用程序生成以终止执行任何其他管理应用程序的终止命令之前拦截所述终止命令,终止执行任何其他管理应用程序包括终止执行所述第二管理应用程序,由此所述操作系统不终止执行所述客户端设备上的所述第二管理应用程序;在所述操作系统接收到所述终止命令之前拦截由所述第一管理应用程序生成以终止执行任何其他管理应用程序的终止命令,终止执行任何其他管理应用程序包括终止执行所述第二管理应用程序,由此所述操作系统不终止执行所述客户端设备上的所述第二管理应用程序;以及响应于所述终止命令被拦截,使所述客户端设备向所述第一管理应用程序传送欺骗响应,就好像所述终止命令已经被所述操作系统接收到一样。

[0008] 本发明还涉及一种计算机可读介质,具有程序代码,所述程序代码在被执行时,使得客户端设备执行上述方法。

[0009] 本发明又涉及一种提供第一管理应用程序和第二管理应用程序两者在客户端设备上的执行的系统,包括:包括硬件处理器的所述客户端设备;以及在所述客户端设备中可

执行的程序指令,当其被所述客户端设备执行时,使得所述客户端设备执行上述方法。

附图说明

[0010] 参考以下附图可以更好地理解本发明的许多方面。附图中的组件不一定按比例缩放,而是重点在于清楚地说明本公开的原则。此外,在附图中,相同的参考数字在几个视图中指代相应的部分。

[0011] 图1是包括管理服务、注册服务和客户端设备的联网环境的图。

[0012] 图2A和图2B是在其上存储有遗留管理应用程序和管理应用程序的客户端设备的原理图的图。

[0013] 图3是说明了由联网环境的组件实现的功能的流程图。

[0014] 图4是说明了由联网环境的组件实现的功能的流程图。

[0015] 图5是说明了由联网环境的组件实现的功能的流程图。

[0016] 图6是说明了由联网环境的组件实现的功能的流程图。

具体实施方式

[0017] 本公开的各个方面涉及设备上多个管理应用程序的共存、设备注册的自动化以及单个设备上多个用户的注册管理。

[0018] 在一些情况下,在单个实例中,管理员从第一类型的管理应用程序转换到另一个可能存在问题。例如,从遗留(legacy)管理应用程序到新的管理应用程序的转换可能会出现许多问题。例如,每个管理应用程序所覆盖的设备管理策略可能不同。在一个设备上同时存在两个管理应用程序,而对较遗留管理应用程序的依赖被逐步淘汰,这可能会有所帮助。但是,特定的遗留管理应用程序(如SCCM)会阻止其他管理应用程序在同一设备上执行管理功能。例如,如果在具有SCCM的设备上安装了新的管理应用程序,则SCCM以编程方式请求该设备的操作系统终止执行新的管理应用程序。因此,在单个设备上拥有两个管理应用程序仍然存在问题。

[0019] 根据一个示例,客户端设备可以配置为识别安装在客户端设备上的第一管理应用程序(例如,遗留管理应用程序)对客户端设备的操作系统具有管理权限,其中第一管理应用程序配置为响应于检测到第二管理应用程序(例如,新安装的管理应用程序)而生成终止命令。在操作系统接收到命令之前,可以拦截该终止命令,这样操作系统就不终止在客户端设备上执行第二管理应用程序。

[0020] 终止命令可以被例如第二管理应用程序、休眠(sleeper)代理应用程序或安装在客户端设备上的、过滤第一管理应用程序发出的预定义的应用程序编程接口(API)调用的驱动程序之一拦截。响应于拦截到终止命令,响应可以被传送给第一管理应用程序,就好像操作系统已经接收到终止命令一样,该过程被称为“欺骗”。此外,当管理员希望从使用第一管理应用程序完全转移到第二管理应用程序时,可以从客户端设备卸载或删除第一管理应用程序。

[0021] 接下来,在一些情况下,企业可以要求其员工、承包商、客户或其他人员将BYOD设备注册到管理服务,管理服务在设备上实施策略,以防止数据被盗、数据丢失和未经授权的访问。使人员下载、安装和配置将设备注册到管理服务的管理应用程序可能会很复杂和存

在问题。因此,许多企业在将设备提供给员工之前,都有管理员对设备进行配置。设备的配置可以通过对设备进行服务开通(provisioning)或使用图像管理来完成,其中新的图像被安装到设备上。服务开通可用于配置设备而无需安装图像。例如,服务开通允许管理员在将设备提供给终端用户之前,使用应用程序、策略和其他材料组织(stage)“收缩包装的”设备。在本文所述的示例中,管理员可以对设备进行服务开通,以便在设备被终端用户接收和访问时,自动将设备注册到管理服务,而终端用户不必在管理应用程序中提供登录凭证。相反,可以使用操作系统的登录凭证。

[0022] 在一个示例中,管理员可以通过在设备上安装管理应用程序来为终端用户对设备进行服务开通。一旦管理应用程序被执行,管理应用程序可以识别执行管理应用程序的用户是临时用户(staging user),例如管理员或对设备进行服务开通的其他用户。管理应用程序可以生成事件监听器,其监控通过客户端设备的操作系统执行的用户账户的至少一个后续登录。例如,当终端用户接收到设备时,事件监听器将监控终端用户执行的到操作系统的登录。在随后的登录中,事件监听器可以识别域和用户名,并将其传送至管理服务以注册设备。例如,计算环境可以使用域来识别企业账户并生成新的用户账户,或者为终端用户定位现有的用户账户。唯一地识别设备的标识符可以与用户账户相关联地存储在数据存储中。

[0023] 参考图1,示出了联网环境100的示例。联网环境100可以包括通过网络109彼此通信的计算环境103和客户端设备106a...106b。例如,网络109可以包括因特网、内联网、外联网、广域网(WAN)、局域网(LAN)、有线网络、无线网络、其他合适的网络或者两个或更多此类网络的任意组合。例如,网络可以包括卫星网络、有线网络、以太网、电话网络和其他类型的网络。

[0024] 计算环境103可包括例如服务器计算机或提供计算能力的任何其他系统。或者,计算环境103可以包括多个计算设备,这些计算设备被布置在一个或更多个服务器库、计算机库或其他布置中。计算环境103可以包括网格计算资源或任何其他分布式计算布置。计算设备可以位于单个安装中,也可以分布在许多不同的地理位置。计算环境103还可以包括或被操作作为一个或更多个虚拟化计算机实例。为了方便起见,本文以单数形式提及计算环境103。尽管计算环境103以单数形式被提及,但应理解,可以在上述各种布置中使用多个计算环境103。由于计算环境103通过网络109与客户端设备106远程通信,因此计算环境103可以被描述为“远程”计算环境103。

[0025] 计算环境103可以包括数据存储112。数据存储112可以包括计算环境103的存储器、计算环境103的大容量存储资源或计算环境103可以在其上存储数据的任何其他存储资源。例如,存储在数据存储112中的数据可以与下面描述的各种应用程序或功能实体的操作相关联。

[0026] 在计算环境103上执行的组件可以包括例如管理服务115、注册服务118以及本文未详细讨论的其他应用程序、服务、过程、系统、引擎或功能。可以执行管理服务115来监督客户端设备106向管理服务115注册的操作。在一些实施例,企业(例如一个或更多个公司或其他组织)可以操作管理服务115来监督或管理其员工、承包商、客户或在管理服务115中拥有用户账户的其他用户的客户端设备106的操作。

[0027] 管理服务115可以使各种软件组件被安装在客户端设备106上。例如,这些软件组

件可以包括例如客户端应用程序121、资源、资源库、驱动程序、设备配置,或者管理服务115的管理员指定的需要在客户端设备106上安装的其他类似组件。管理服务115可以进一步使得在客户端设备106上实现策略。

[0028] 策略可以包括,例如,与客户端设备106的能力相关的限制或权限,以便在客户端设备106上保护对企业数据的访问。例如,策略可以包括在预定义的时间窗口(例如,上午9:00到下午5:00)期间,当客户端设备106位于办公楼的特定位置时,提供对企业数据的访问。此外,策略还可以包括在客户端设备106不在办公楼的位置或在预定义的时间窗口的时间之外时拒绝对企业数据的访问。策略还可以包括启用或禁用客户端设备106上的某些功能。在一个示例中,当客户端设备106位于特定位置时,策略可以拒绝摄像机或录音功能。可以理解的是,还可以实现其它策略。管理员可以根据企业的兴趣或安全策略配置策略。

[0029] 管理服务115可以与在客户端设备106上执行的一个或更多个客户端应用程序121交互。在一个示例中,管理服务115与客户端设备106上的管理应用程序124交互,以将客户端设备106注册到管理服务115。注册后,管理应用程序124可以被注册为客户端设备106的设备管理员,其可以为管理应用程序124提供足够的权限来控制客户端设备106的操作。在一个示例中,通过在客户端设备106的操作系统上安装管理配置文件,可以将管理应用程序124注册为设备管理员,其使得客户端设备106的操作系统127a...127b指定管理应用程序124为设备管理员。

[0030] 管理服务115可以引导管理应用程序124在客户端设备106上执行设备管理功能。例如,管理服务115可以引导管理应用程序124控制对客户端设备106上可用的某些软件或硬件功能的访问。因此,管理服务115可以验证客户端设备106的配置和操作符合预先定义的标准,该标准确保企业数据或其他数据被保护而不受到数据丢失、未经授权访问或其他有害事件。

[0031] 管理服务115可以通过管理应用程序124进一步向客户端设备106提供企业数据130。在一个示例中,管理服务115可以通过使用管理服务115提供的命令队列,使管理应用程序124控制客户端设备106的使用,或向客户端设备106提供企业数据130。在一些示例中,管理服务115可以将命令存储在与特定客户端设备106相关联的命令队列中,并且可以配置客户端设备106执行的管理应用程序124以检索命令队列的内容。在另一个示例中,管理应用程序124可以被配置为在配置好的间隔(例如每四小时)上检索命令队列的内容,或者在检测到特定事件(例如检测到客户端设备106正在执行未经授权的应用程序)时检索命令队列的内容。

[0032] 在任何情况下,管理应用程序124都可以通过登记(check in)到管理服务115并请求命令队列的内容来检索命令队列的内容。在一个示例中,命令队列的内容可以包括应使得管理应用程序124在客户端设备106上执行的命令。在另一个示例中,命令队列的内容可以包括资源或客户端应用程序121,应使得管理应用程序124被安装在客户端设备106上,客户端设备106可以通过指定的统一资源定位符(URL)对其进行访问。

[0033] 注册服务118被执行以将客户端设备106注册到管理服务115,这样管理服务115可以监督客户端设备106的配置和管理。为此,注册服务118可以为客户端设备106的用户维护用户账户数据133。用户账户数据133可以包括例如用户名、电子邮件地址、密码、生物识别信息或其他身份验证数据。此外,注册服务118可以维护唯一地识别用户账户的客户端设备

106的识别符136a...136b的映射。

[0034] 存储在数据存储112中的数据可以包括,例如,管理服务数据139、设备数据142、企业数据130和用户账户数据133以及其他数据。管理服务115包括与注册到管理服务115的客户端设备106的管理相关的信息。为此,管理服务数据139可以包括例如标识符136、配置文件145、合规规则148以及其他数据。

[0035] 配置文件145包括管理服务115的管理员为配置客户端设备106中的各个设备而指定的设置。例如,配置文件145可以指示要安装在客户端设备106上的特定客户端应用程序121、驱动程序或其他软件组件。此外,配置文件145可以包括客户端设备106的其他设置。客户端设备106的配置可以由管理应用程序124执行,如适用的配置文件145所指定的。通过管理员控制台,管理员可以为客户端设备106、一组客户端设备106或用户组152创建配置文件145。可以理解,一些客户端设备106的配置与其他客户端设备106可以不同。在一些示例中,配置文件145可以包括可扩展标记语言(XML)文档或其他适当类型的文件,这些文件可以被传送到客户端设备106或由管理应用程序124访问。

[0036] 合规规则148可以包括用于使客户端设备106“符合”管理服务115而由管理员指定的约束条件。合规规则148可以包括管理员指定的标准或其他标准。在一个示例中,管理应用程序124可以配置客户端设备106的硬件或软件功能,以使客户端设备106符合合规规则148。例如,管理员可以指定自动安装在客户端设备106上的特定类型的软件更新。此外,管理应用程序124可以识别客户端设备106何时不符合合规规则148以及其他策略,并可以采取适当的补救措施,例如拒绝访问企业数据130、拒绝安装软件更新或管理应用程序124的其他特征。

[0037] 在一些示例中,管理服务115与管理应用程序124或可在客户端设备106上执行的其他客户端应用程序121通信,以确定客户端设备106上是否存在不满足合规规则148的漏洞(vulnerability)。漏洞可以包括,例如,客户端设备106上存在病毒或恶意软件、客户端设备106被“寻根(rooted)”或“越狱(jailbroken)”,其中根访问被提供给客户端设备106的用户、特定应用程序或文件的存在、有问题的设备配置、客户端应用程序121的有漏洞版本或其他可以理解的漏洞。

[0038] 设备数据142可以包括,例如,与客户端设备106的各个设备的注册状态155相关的数据。在一个示例中,被指定为“已注册”的客户端设备106被允许访问企业数据130,而被指定为“未注册”、没有被指定、或“已注册”但不符合合规规则148的客户端设备106可以被拒绝对企业数据130的访问。设备数据142还可以包括与用户组152相关的数据,其可以包括属于组织单位的客户端设备106的组,例如信息技术(IT)、销售、营销或企业或组织的其他适当安排。管理员可以通过管理员控制台指定属于特定用户组152的一个或更多个客户端设备106。

[0039] 客户端设备106可以代表一个或更多个客户端设备106。客户端设备106可以包括基于处理器的系统,例如计算机系统,该系统可以包括台式计算机、笔记本电脑、个人数字助理、移动电话、智能手机、机顶盒、音乐播放器、平板电脑系统、游戏机、电子图书阅读器或任何其他具有类似功能的设备。客户端设备106还可以配备有联网能力或联网接口,包括本地化联网或通信能力,例如近场通信(NFC)能力、射频识别(RFID)读写能力或其他本地化通信能力。

[0040] 客户端设备106可以包括操作系统127,配置为执行各种客户端应用程序121,例如管理应用程序124、遗留管理应用程序158或其他应用程序。客户端设备106还可以包括驱动程序,例如设备驱动程序或软件驱动程序,这些驱动程序操作或控制耦合到客户端设备106或安装在其上的软件的硬件设备。驱动程序可以包括由管理应用程序124安装的过滤器驱动程序161,如前所述。一些客户端应用程序121可以访问由计算环境103或其他服务器提供服务的网络内容,从而在显示器172(例如液晶显示器(LCD)、触摸屏显示器或其他类型的显示设备)上呈现用户界面169。为此,一些客户端应用程序121可以包括浏览器或专用应用程序,并且用户界面可以包括网络页面、应用程序屏幕或其他界面。此外,其他客户端应用程序121可以包括设备管理应用程序、企业应用程序、社交网络应用程序、文字处理器、电子表格应用程序、媒体查看应用程序或其他应用程序。

[0041] 接下来,提供了对联网环境100的各个组件的操作的一般性描述。在一些情况下,企业可能希望从第一类管理应用程序转移到另一类管理应用程序。例如,企业可能希望逐步停止使用由一个实体操作的遗留管理应用程序158,而使用由第二实体操作的管理应用程序124。从客户端设备106中删除遗留管理应用程序158并在单个实例中安装管理应用程序124可能存在问题,因为客户端设备106在转移期间可能有漏洞,或者由于与遗留管理应用程序158与管理应用程序124实现的不同策略相关联的复杂性。因此,在客户端设备106上同时存在遗留管理应用程序158和管理应用程序124两者,同时逐步停止使用遗留管理应用程序158,这是有益的。但是,特定类型的传统管理应用程序158(如SCCM)会阻止其他管理应用程序在客户端设备106上执行管理功能。例如,如果管理应用程序124安装在具有SCCM的设备上,SCCM以编程方式请求客户端设备106的操作系统127定期或在检测到管理事件时终止管理应用程序124的执行。

[0042] 因此,可以将安装在客户端设备106上的管理应用程序124配置为识别在客户端设备106上安装有遗留管理应用程序158,并且其具有对客户端设备106的操作系统127的管理权限。如上所述,遗留管理应用程序158可以例如通过定期生成终止命令或响应于检测到管理应用程序124来阻止管理应用程序124对客户端设备106的操作。

[0043] 因此,在操作系统127接收到命令之前,管理应用程序124可以拦截由遗留管理应用程序158生成的终止命令,以便操作系统127不终止执行管理应用程序124。在一个例子中,终止命令可以被管理应用程序124中的一个拦截。在另一个示例中,可以在客户端设备106上安装休眠代理应用程序或过滤器驱动程序161,以监控遗留管理应用程序158发出的预定义的API调用,其中所述API调用用于指示操作系统127或其他组件终止管理应用程序124的执行。

[0044] 管理应用程序124、休眠代理应用程序或过滤器驱动程序161中的一个可以生成并传送对遗留管理应用程序158的响应,就像操作系统127已接收到终止命令一样。此外,当管理员希望从使用遗留管理应用程序158完全转移到使用管理应用程序124时,可以通过管理应用程序124从客户端设备106卸载或删除遗留管理应用程序158。

[0045] 此外,在将客户端设备106装货或以其它方式提供给人员之前,许多企业都有管理员对它们进行配置。可以使用服务开通或图像管理对客户端设备106进行配置。图像管理通常包括在客户端设备106上安装预配置的图像,然后将客户端设备106提供给人员。但是,定制的级别较低,因为必须为每个不同的配置生成新的图像。另一方面,服务开通可用于配置

设备而无需生成图像。例如,服务开通允许管理员在将客户端设备106提供给终端用户之前,使用客户端应用程序121、策略、资源和其他材料组织收缩包装的设备。在一些示例中,客户端设备106可由企业或管理服务115的管理员提供,以便在被终端用户接收和访问时,将客户端设备106自动地注册到管理服务115。在这种情况下,终端用户没有通过管理应用程序124提供登录凭证或其他复杂信息(如域、互联网协议(IP)地址或类似信息)来注册到注册服务118。相反,可以采用操作系统127的登录凭证,如图1的客户端设备106a所示。

[0046] 在一个示例中,管理员可以通过在客户端设备106上安装管理应用程序124来为终端用户开通客户端设备106的服务。管理应用程序124一旦执行,管理应用程序124可以识别操作系统127的当前用户,并通过与计算环境103的通信,确定执行管理应用程序124的用户是临时用户(staging user),例如管理员或对设备进行服务开通的其他用户。管理应用程序124可以在客户端设备106中创建事件监听器180,其监控通过客户端设备的操作系统127执行的用户账户的至少一个后续登录。例如,当客户端设备106被终端用户接收时,事件监听器180可以监控终端用户执行的登录到操作系统127。例如,如图1的用户界面169所示,在向终端用户提供操作系统127的桌面或客户端设备106的其他特征的访问之前,操作系统127可以要求终端用户提供用户名、密码或其他信息。

[0047] 在登录期间,事件监听器180可以识别域183a...183b和用户句柄(user handle) 186a...186b,并将其传送至注册服务118,以便使用管理服务115注册客户端设备106。例如,注册服务118可以使用域183从数据存储112中识别对应于企业、组织或其他实体的企业账户。使用企业账户,注册服务118可以从用户账户数据133中定位终端用户的现有用户账户或生成新的用户账户。事件监听器180还可以访问标识符136,该标识符136唯一地识别可以与用户账户相关联地存储在数据存储112中的客户端设备106。在一个示例中,标识符136是从操作系统127的注册表中获得的。

[0048] 接下来参考图2A和图2B,其示出了说明了单个客户端设备106上的多个管理应用程序的示意结构200a、200b。首先参考图2A,示出了在其上安装有遗留管理应用程序158和管理应用程序124的客户端设备106。然而,遗留管理应用程序158可被配置为通过定期生成终止命令203或响应于检测到管理应用程序124来阻止管理应用程序124在客户端设备106上的操作。例如,终止命令203可以包括例如API调用或函数调用。例如,终止命令203可以包括终止进程()或类似的函数:

```
        BOOL WINAPI TerminateProcess(  
            _In_ HANDLE hProcess,  
[0049]        _In_ UINT    uExitCode  
        );
```

[0050] 一旦接收到终止命令203,操作系统127可以终止管理应用程序124的执行。此后,操作系统127可以向遗留管理应用程序158发送响应206。例如,响应206可以指示管理应用程序124的执行已被成功终止。

[0051] 参考图2B,管理应用程序124可以在客户端设备106上安装过滤器驱动程序161。在一些示例中,在操作系统127接收到终止命令203之前,过滤器驱动程序161可以拦截由遗留管理应用程序158生成的终止命令203。因此,与图2A中描述的场景相反,操作系统127不终

止管理应用程序124的执行。在其他示例中,终止命令203可以被安装在客户端设备106上的管理应用程序124或休眠代理应用程序拦截。休眠代理应用程序可以包括后台进程或服务(类似于过滤器驱动程序161),其监控由遗留管理应用程序158进行的预定义API调用。例如,休眠代理应用程序可以监控用于指示操作系统127或其他组件终止管理应用程序124的执行的API调用。

[0052] 过滤器驱动程序161可以生成欺骗响应209,并将其传送至遗留管理应用程序158,就好像操作系统127已接收到终止命令并成功完成一样。此外,当管理员希望从遗留管理应用程序158的使用完全转移到管理应用程序124时,可以通过管理应用程序124从客户端设备106卸载或删除遗留管理应用程序158。在一个示例中,管理应用程序124可以生成命令行参数(argument),其指示操作系统127启动对遗留管理应用程序158的删除。

[0053] 继续到图3,示出了流程图,该流程图提供了客户端设备106的一部分的操作的一个示例,以提供遗留管理应用程序158和管理应用程序124的共存。根据一个或更多个示例,图3的流程图可以视为描述管理应用程序124、休眠代理应用程序或其他合适的软件组件实现的方法的元素的示例。本文所讨论的功能的分离或分割仅用于说明目的。

[0054] 在步骤303中,客户端设备106可以识别安装在客户端设备106上的第一管理应用程序的存在。例如,第一管理应用程序可以包括例如遗留管理应用程序158。由于某些遗留管理应用程序158(例如SCCM)阻止管理应用程序124(或其他类似的客户端应用程序121)在客户端设备106上的操作,因此管理应用程序124可以为第一管理应用程序和第二管理应用程序(例如管理应用程序124)实现措施,以在客户端设备106上共存。

[0055] 接下来,在步骤306中,管理应用程序124可以在客户端设备106上安装过滤器驱动程序161,以监控第一管理应用程序所执行的API调用。例如,过滤器驱动程序161可以监控由第一管理应用程序生成的终止命令203。

[0056] 在步骤309中,在操作系统127接收到终止命令203之前,过滤器驱动程序161可以拦截由第一管理应用程序生成的终止命令203。因此,操作系统127将不终止管理应用程序124的执行。在其他示例中,终止命令203可以被安装在客户端设备106上的管理应用程序124或休眠代理应用程序中的一个拦截。

[0057] 在步骤312中,过滤器驱动程序161或其他组件可以生成欺骗响应209,并将其传送给遗留管理应用程序158,就像操作系统127已经在成功终止第二管理应用程序后生成了终止命令203一样。第二管理应用程序可以与客户端设备106上的第一管理应用程序一起继续操作。

[0058] 在步骤315中,如果需要的话,第一管理应用程序(诸如,遗留管理应用程序158)可以由管理应用程序124从客户端设备106中卸载或删除,例如,当企业希望从使用第一管理应用程序完全转移到使用第二管理应用程序时。在一个示例中,管理应用程序124可以生成命令行参数,其指示操作系统127启动对遗留管理应用程序158的删除。此后,该过程可继续完成。

[0059] 继续到图4,示出了提供客户端设备106的一部分的操作的一个示例以提供客户端设备106的自动注册的流程图。根据一个或更多个示例,图4的流程图可以被视为描述管理应用程序124或其他合适的软件组件实现的方法的元素的示例。本文所讨论的功能的分离或分割仅用于说明的目的。

[0060] 可以使用服务开通来配置客户端设备106,以便当终端用户接收到它们时,登录到客户端设备106的操作系统127会导致客户端设备106自动注册到管理服务115。在这种情况下,终端用户没有提供登录凭证或其他复杂的数据。相反,可以采用操作系统127的登录凭证。在一个示例中,管理员可以通过在客户端设备106上安装管理应用程序124来为终端用户开通客户端设备106的服务。

[0061] 在步骤403中,管理应用程序124可以识别操作系统127的当前用户,以确定例如操作系统127的当前用户是临时用户还是终端用户,例如客户端设备106的预期接收者。

[0062] 在步骤406中,客户端设备106可以确定当前用户是否是临时用户,例如管理员或对客户端设备106进行服务开通的其他用户。在一个示例中,客户端设备106所识别的当前用户可以被传送至计算环境103,并与已批准的管理员的白名单进行比较。如果当前用户不是临时用户,则流程可以继续完成。

[0063] 或者,如果当前用户是临时用户,则过程可以进行到步骤409。在步骤409中,管理应用程序124可以创建事件监听器180,其监控通过客户端设备106的操作系统127执行的用户账户的一个或更多个后续登录。例如,当终端用户接收到客户端设备106时,事件监听器180可以监控终端用户执行的登录到操作系统127。如图1的用户界面169所示,在向终端用户提供访问操作系统127的桌面或客户端设备106的其他特征之前,操作系统127可以要求终端用户提供用户名、密码或其他信息。

[0064] 在步骤412中,事件监听器180可以确定是否已执行后续登录。例如,后续登录可以包括例如终端用户的初始登录,而不是管理员或对客户端设备106进行服务开通的其他用户的后续登录。为此,在一些示例中,事件监听器180可以确定用户名是否不存在于管理员或其他被批准对客户端设备106进行服务开通的人员的白名单中。如果尚未执行后续登录,则可以继续完成该过程。

[0065] 或者,如果已执行后续登录,则过程可以进行到步骤415。在一些示例中,用户名可以包括域183和用户句柄186。在步骤415中,在通过操作系统127登录期间,事件监听器180可以识别域183和用户句柄186。例如,参照图1,域183可以包括“企业”,而用户句柄186包括“史密斯_约翰”。域183可以表示管理服务115所管理的特定企业账户。

[0066] 在步骤418中,客户端设备106可以从客户端设备106的注册表访问与域183和用户句柄186相关联的标识符136。标识符136可以例如与操作客户端设备106的用户相关联地唯一地识别客户端设备106。

[0067] 在步骤421中,客户端设备106可以将标识符136、域183和用户句柄186发送到计算环境103以自动注册客户端设备106。例如,注册服务118可以使用域183从数据存储112中识别对应于企业、组织或其他实体的企业账户。使用企业账户,注册服务118可以从用户账户数据133中定位终端用户的现有用户账户或生成新的用户账户。标识符136可以与用户账户关联地存储,以便客户端设备106在之后可以被管理服务115识别。例如,标识符136可用于客户端设备106的用户的后续身份验证。此后,该过程可继续到完成。

[0068] 现在转到图5,示出了提供计算环境103的一部分的操作的一个示例以提供客户端设备106的自动注册的流程图。图5的流程图可以视为根据一个或更多个示例描述管理服务115、注册服务118或其他合适的软件组件所实现的方法的元素的示例。本文所讨论的功能的分离或分割仅用于说明的目的。

[0069] 在步骤503中,计算环境103可以从客户端设备106接收标识符136、域183和用户句柄186,例如,以将客户端设备106注册到管理服务115。如上所述,客户端设备106可以识别在客户端设备106上执行的后续登录,例如,在管理员在对客户端设备106进行服务开通之后。客户端设备106可以使用通过操作系统127登录提供的信息来自动注册客户端设备106。

[0070] 在步骤506中,计算环境103可以使用域183从数据存储112中查找与企业、组织或其他实体对应的企业账户。例如,计算环境103可以使用域183生成搜索查询并在数据存储112中执行。

[0071] 接下来,在步骤509中,计算环境103可以使用例如域183和用户句柄186从用户账户数据133中查找终端用户的现有用户账户。例如,如图1的用户界面169所示,用户句柄186“史密斯_约翰”可用于识别企业账户的终端用户约翰史密斯的用户账户。

[0072] 在步骤512中,标识符136可以与用户账户关联地存储,以便稍后管理服务115可以识别客户端设备106。例如,标识符136可用于客户端设备106的用户的后续身份验证。

[0073] 在步骤515中,可以在数据存储112中更新注册状态155。例如,注册状态155可以被更新为“已注册”。在其他示例中,可以更新注册状态155以反映客户端设备106已登记到管理服务115,但客户端设备106需要在注册状态更新为“已注册”或“完全注册”之前,由管理应用程序124进行配置。

[0074] 在步骤518中,计算环境103可用于管理或监督客户端设备106的操作。例如,通过经由服务开通预安装在客户端设备106上的管理应用程序124,管理服务115可以使各种软件组件被安装在客户端设备106上。软件组件可以包括,例如,客户端应用程序121、资源、库、驱动程序、设备配置,或者管理服务115的管理员指定的需要在客户端设备106上安装的其他类似组件。管理服务115可进一步使得在客户端设备106上实现策略。例如,策略可以包括与客户端设备106的能力相关的限制或权限,以便在客户端设备106上保护对企业数据的访问。此后,该过程可进行到完成。

[0075] 接下来参照图6,示出了提供客户端设备106的一部分的操作的一个示例以提供客户端设备106上的多个用户设备管理的流程图。图6的流程图可以视为根据一个或更多个示例描述管理应用程序124或其他合适的软件组件实现的方法的元素的示例。本文所讨论的功能的分离或分割仅用于说明的目的。

[0076] 传统上,管理服务115只维护用户账户到客户端设备106的映射。例如,数据存储112可以包括唯一地识别客户端设备106的标识符136。但是,在许多情况下,客户端设备106可以在多个用户之间共享。例如,拥有多个员工的团队可以共享单个客户端设备106。与在单个客户端设备106上管理单个用户相比,管理每个用户的客户端设备106的操作是有益的。

[0077] 从步骤603开始,客户端设备106可以识别通过操作系统127执行的第一用户的登录。例如,操作系统127可以要求用户提供用户名和密码以登录到桌面环境或操作系统127提供的其他形式的会话。在一些示例中,管理应用程序124可以使用操作系统127提供的一个或更多个API来查询操作系统127,以识别用户登录事件,或识别操作系统127的活动用户。

[0078] 接下来,在步骤606中,管理应用程序124至少部分基于第一用户和客户端设备106配置客户端设备106。例如,数据存储112可以为客户端设备106的每个活动用户维护管理服务

务115的用户账户的映射。映射可用于访问企业数据130、配置文件145、合规规则148或适用于第一用户的其他信息。例如，映射可以包括唯一地识别客户端设备106和客户端设备106的用户的标识符136。在一个示例中，映射可以类似于下表结构：

[0079]	行_编号	用户_账户_Id	OS_用户_Id	设备_Id
	...	...	...	...
	105896	AXY876	846X2A	41350X

[0080] 表1

[0081] 其中“用户_账户_Id”包括唯一地识别管理服务115的用户账户的标识符136，“OS_用户_Id”包括唯一地识别客户端设备106的活动用户的标识符136，“设备_Id”包括唯一地识别客户端设备106的标识符136。“用户_账户_Id”可用于识别用于管理客户端设备106或提供对企业数据130的访问的其他数据。

[0082] 接下来，在步骤609中，管理应用程序124可以为第一用户管理客户端设备106。例如，管理应用程序124可以基于包含第一用户的用户组152来监督客户端设备106的操作。例如，这可以包括例如根据一个或更多个适用的配置文件145限制客户端设备106上的功能，为第一用户提供企业数据130，验证客户端设备106是否符合一个或更多个合规规则148，或执行另一个设备管理功能，如能够领会的那样。

[0083] 接下来，在步骤612中，客户端设备106可以确定用户是否已变更。例如，第一用户可以注销操作系统127，随后第二用户可以使用与第一用户不同的用户名和密码登录操作系统127。管理应用程序124可以使用操作系统127的一个或更多个API来识别注销事件以及第二用户执行的后续登录事件。如果未识别到用户的变更，则过程可以恢复到步骤609。或者，如果识别了用户的变更，则过程可以进行到步骤615。

[0084] 在步骤615中，管理应用程序124可以基于操作系统127的第二用户配置客户端设备106，其中第二用户与第一用户不同。例如，第二用户的一个或更多个配置文件145可以被识别，并被用于配置客户端设备106。此外，可以使客户端设备106基于新用户访问适当的企业数据130。

[0085] 在步骤618中，管理应用程序124可以为第二用户管理客户端设备106。在一些示例中，管理应用程序124可以基于包括第二用户的用户组152监督客户端设备106的操作。例如，管理应用程序124可以根据一个或更多个适用的配置文件145限制客户端设备106上的功能，为第二用户提供企业数据130，验证客户端设备106是否符合一个或更多个合规规则148，或者执行另一设备管理功能，如可以领会的那样。此后，该过程可前进到完成。

[0086] 客户端设备106或包含计算环境103的设备可以包括至少一个处理器电路，例如，具有处理器和至少一个存储器设备，这两者分别耦连到本地接口。例如，该设备可以包括例如至少一个计算机、移动设备、智能手机、计算设备或类似设备。例如，本地接口可以包括例如具有附带地址/控制总线或其他总线结构的数据总线。

[0087] 存储在存储器设备中的是处理器可执行的数据和多个组件。特别是，存储在一个或更多个存储器设备中并可由设备处理器执行的可以是客户端应用程序121，也可以是其他应用程序。存储器中还可以存储数据存储112和其他数据。

[0088] 许多软件组件存储在存储器中，并可由处理器执行。在这方面，术语“可执行文件”指的是最终可以由处理器运行的形式的程序文件。可执行程序的例子可以是，例如，可以被

转换成机器代码的编译的程序,其格式为可以被加载到一个或多个存储器设备的随机访问部分中并由处理器运行;可以被表示成例如能够被加载到一个或多个存储器设备的随机访问部分并由处理器执行的目标代码格式的代码;或能够由另一个可执行程序解释以在由处理器执行的存储器设备的随机存取部分中生成指令的代码。可执行程序可以存储在存储器设备的任何部分或组件中,包括随机存取存储器(RAM)、只读存储器(ROM)、硬盘、固态硬盘、USB闪存驱动器、存储卡、光学盘(如光盘(CD)或数字多功能盘(DVD)、软盘、磁带或其他存储组件。

[0089] 存储器可以包括易失性和非易失性存储器以及数据存储组件。此外,处理器可以表示多个处理器和/或多个处理器核,并且一个或多个存储器设备可以分别表示在并行处理电路中运行的多个存储器。存储器设备还可以表示各种类型的存储设备的组合,例如RAM、大容量存储设备、闪存或硬盘存储。在这种情况下,本地接口可以是适当的网络,其辅助多个处理器中的任意两个之间或任何处理器与任何存储器设备之间的通信。本地接口可以包括被设计用于协调此通信的附加系统,包括,例如,执行负载平衡。处理器可以是电气的,也可以是一些其他可用的结构。

[0090] 客户端设备106可以包括显示器172,在该显示器172上可以呈现客户端应用程序121或另一应用程序生成的用户界面169。在一些示例中,可以使用计算环境103提供的用户界面数据生成用户界面169。客户端设备106还可以包括一个或多个输入/输出设备,其可以包括例如电容式触摸屏或其他类型的触摸输入设备、指纹读取器或键盘。

[0091] 尽管管理服务115、客户端应用程序121和本文所述的其他各种系统可以具体化在由上述通用硬件执行的软件或代码中,作为替代方案,同样也可以具体化在专用硬件或软件/通用硬件和专用硬件的组合中。如果具体化在专用硬件中,则每个硬件都可以实现为使用多种技术中的任何一种或多种技术的组合的电路或状态机。这些技术可以包括具有逻辑门的离散逻辑电路,用于在应用一个或多个数据信号时实现各种逻辑功能;具有适当逻辑门的应用特定集成电路(ASIC)、现场可编程门阵列(FPGA)或其他组件。

[0092] 序列图和流程图示出了本文所述部分组件实现的功能和操作的示例。如果具体化在软件中,每个块都可以表示模块、段或代码的一部分,其中可以包括实现一个或多个指定逻辑功能的程序指令。程序指令可以具体化为源代码的形式,其可以包括用编程语言编写的人类可读语句,或具体化为机器代码的形式,其可以包括可由适当的执行系统(诸如计算机系统或其他系统中的处理器)识别的数字指令。机器代码可以从源代码转换。如果具体化为硬件,则每个块可以表示一个电路或多个互连的电路,以实现一个或多个指定的逻辑功能。

[0093] 虽然序列图流程图示出了具体的执行顺序,但可以理解,执行顺序可以与所描述的不同。例如,两个或多个块的执行顺序可以相对于显示的顺序进行置乱。另外,连续示出的两个或多个块可以同时执行,也可以部分同时执行。此外,在一些实施例中,可以跳过或省略图中所示的一个或多个块。

[0094] 此外,本文所述的包括软件或代码的任何逻辑或应用程序可以包含在任何非暂时性计算机可读介质中,供指令执行系统(例如,计算机系统或其他系统中的处理器)使用或与之连接。在这个意义上,逻辑可以包括,例如,包括指令的语句和可以从计算机可读介质中提取并由指令执行系统执行的声明。在本公开的上下文中,“计算机可读介质”可以是包

含、存储或维护本文所述逻辑或应用程序以供指令执行系统使用或与之相关的任何介质。

[0095] 计算机可读介质可以包括许多物理介质(例如磁性、光学或半导体介质)中的任何一种。合适的计算机可读介质的更具体的示例包括固态驱动器或闪存。此外,本文描述的任何逻辑或应用程序都可以多种方式实现和构造。例如,一个或多个应用程序可以作为单个应用程序的模块或组件实现。此外,本文所述的一个或多个应用程序可以在共享或单独的计算设备或其组合中执行。例如,本文所述的多个应用程序可以在同一计算设备或多个计算设备中执行。

[0096] 强调的是,上述本公开的实施例仅仅是为本公开的原则的清楚理解而阐述的实施的可能示例。可以对上述实施例进行许多变更和修改,而不会实质上背离本发明的精神和原则。所有此类修改和变更均应包含在本公开的范围內。

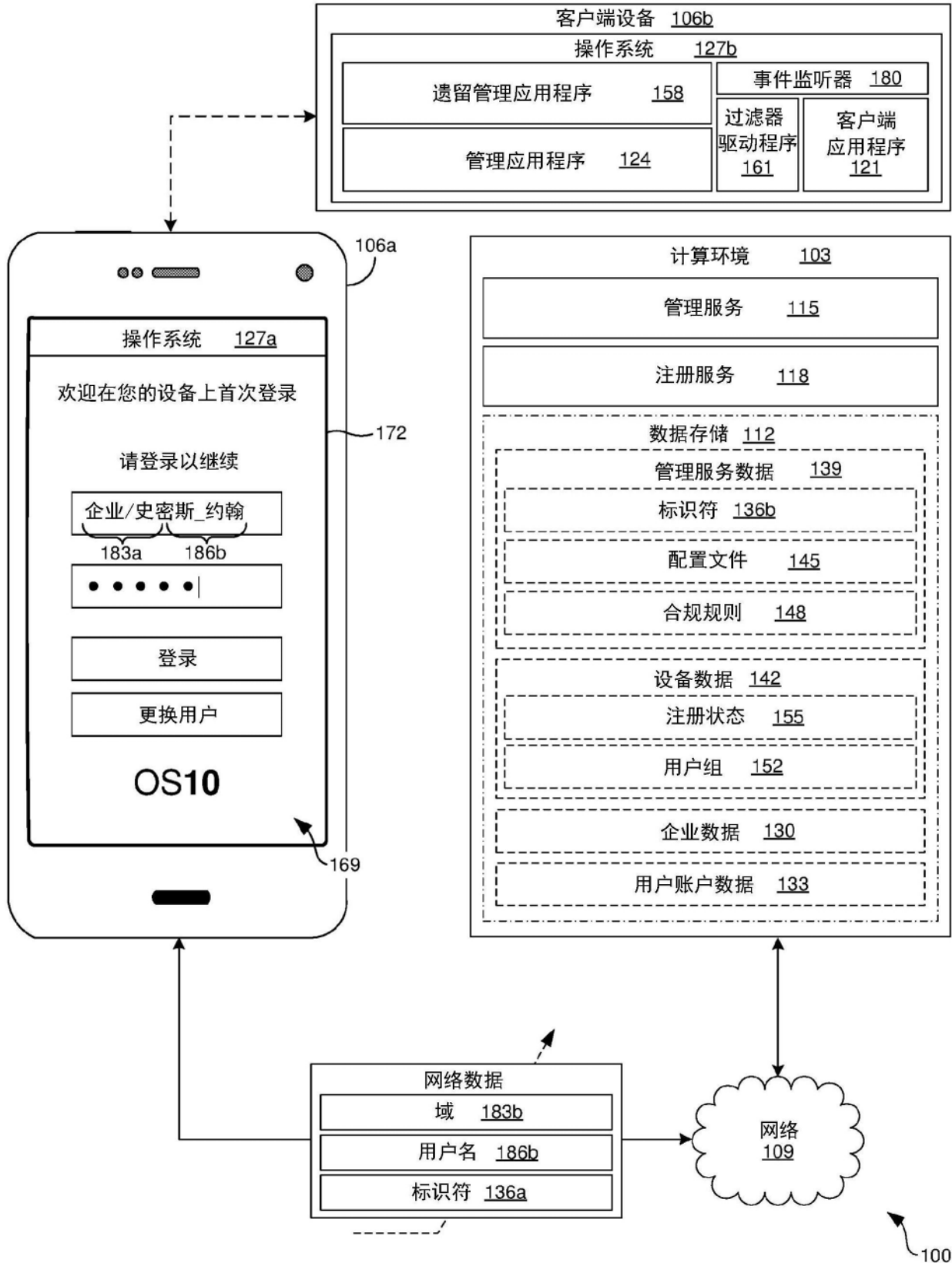


图1

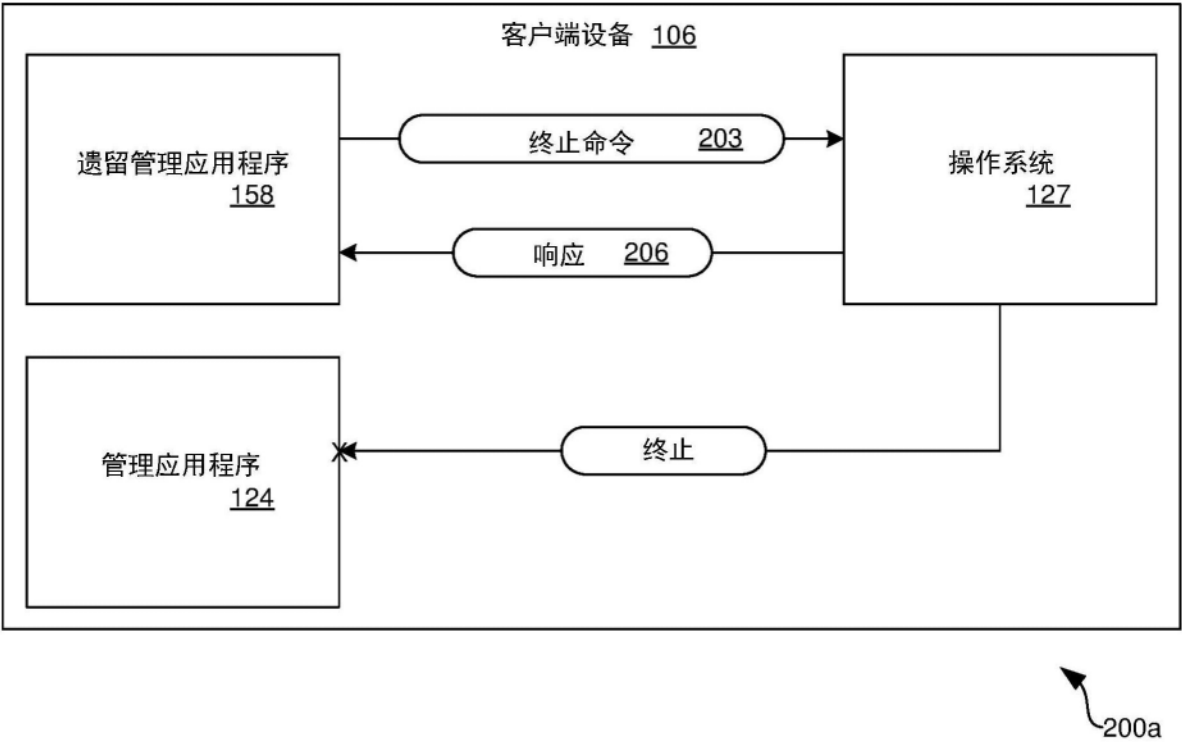


图2A

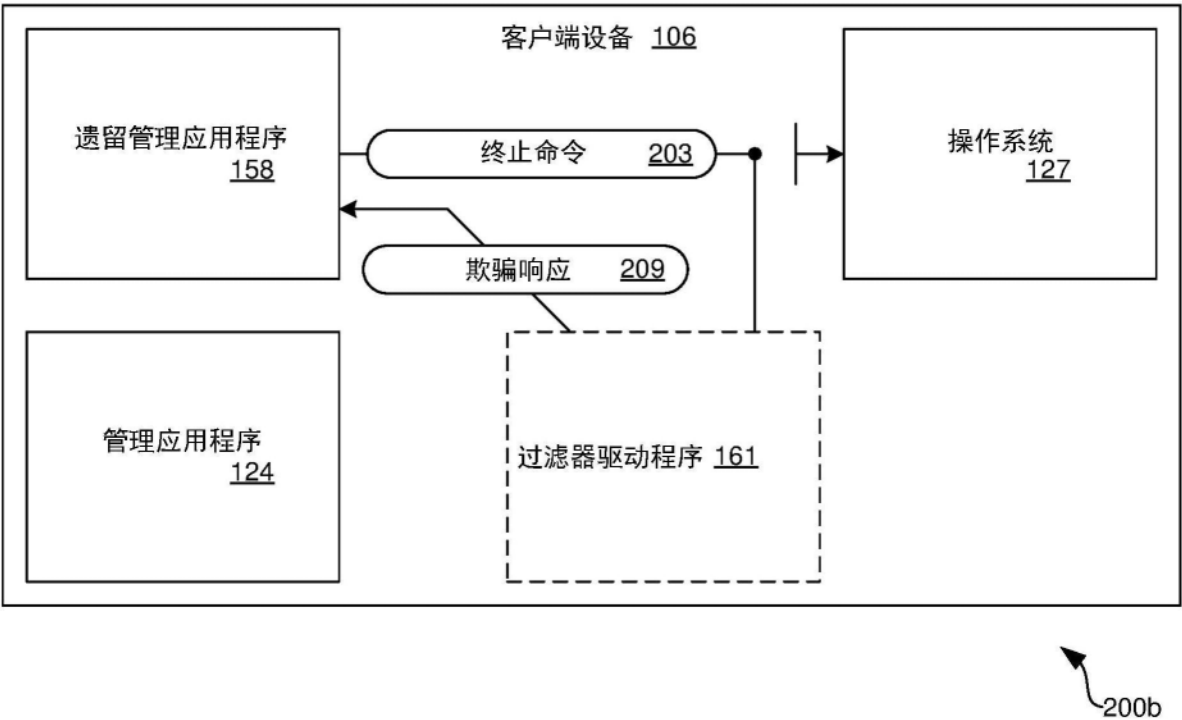


图2B

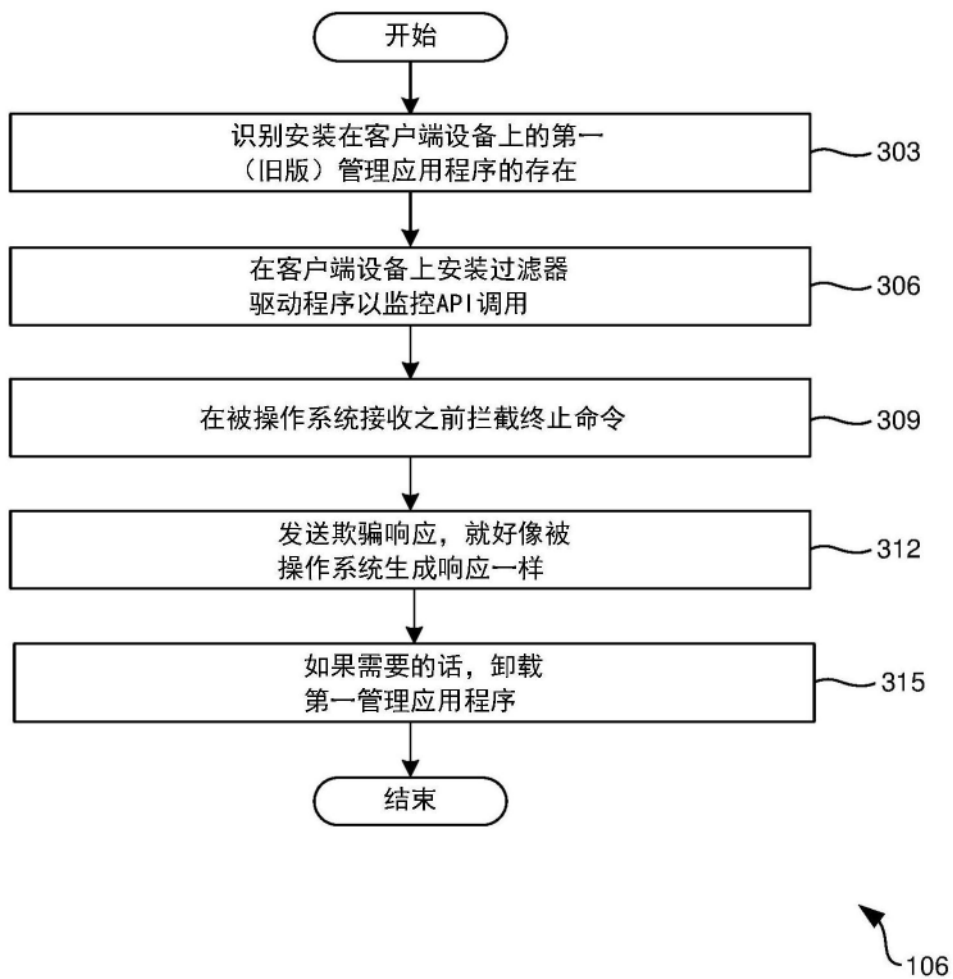


图3

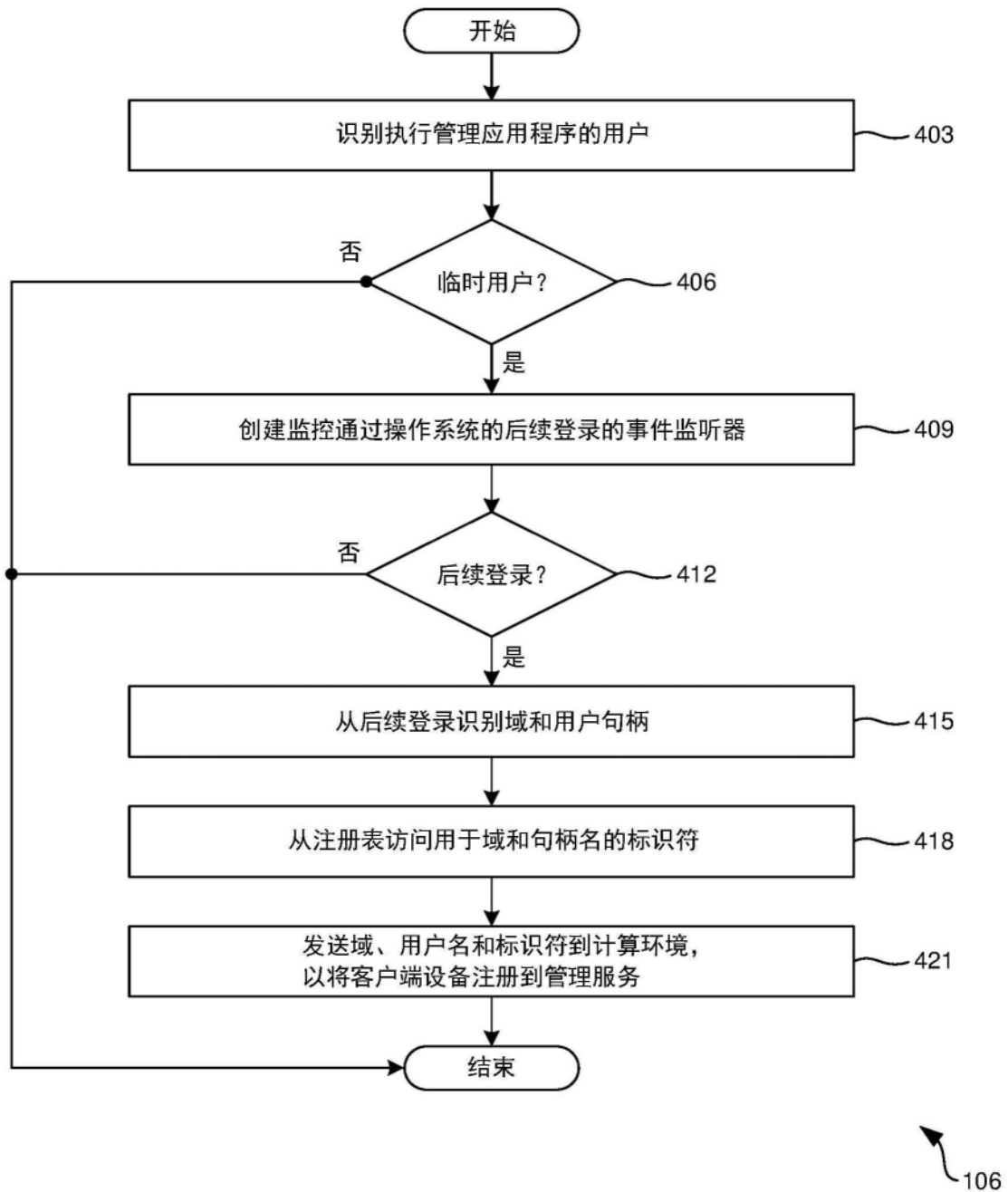


图4

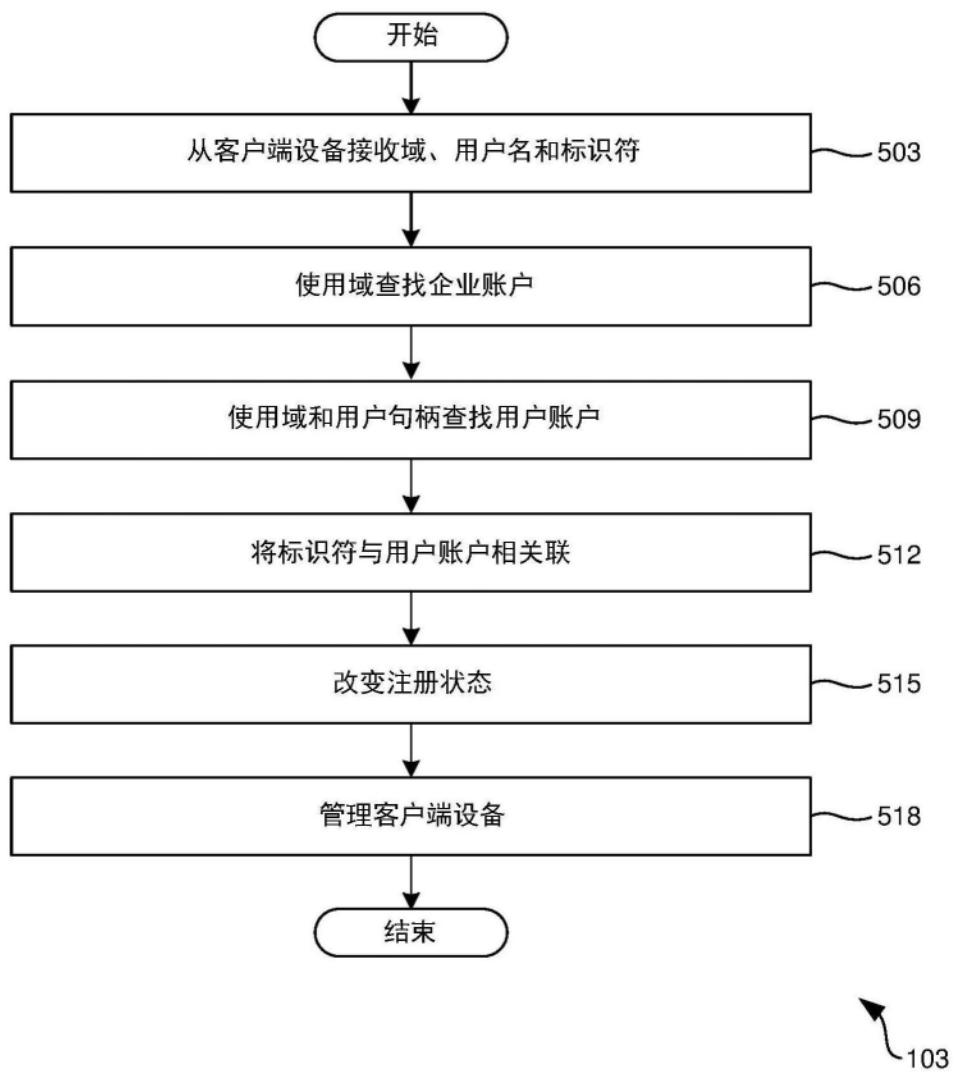


图5

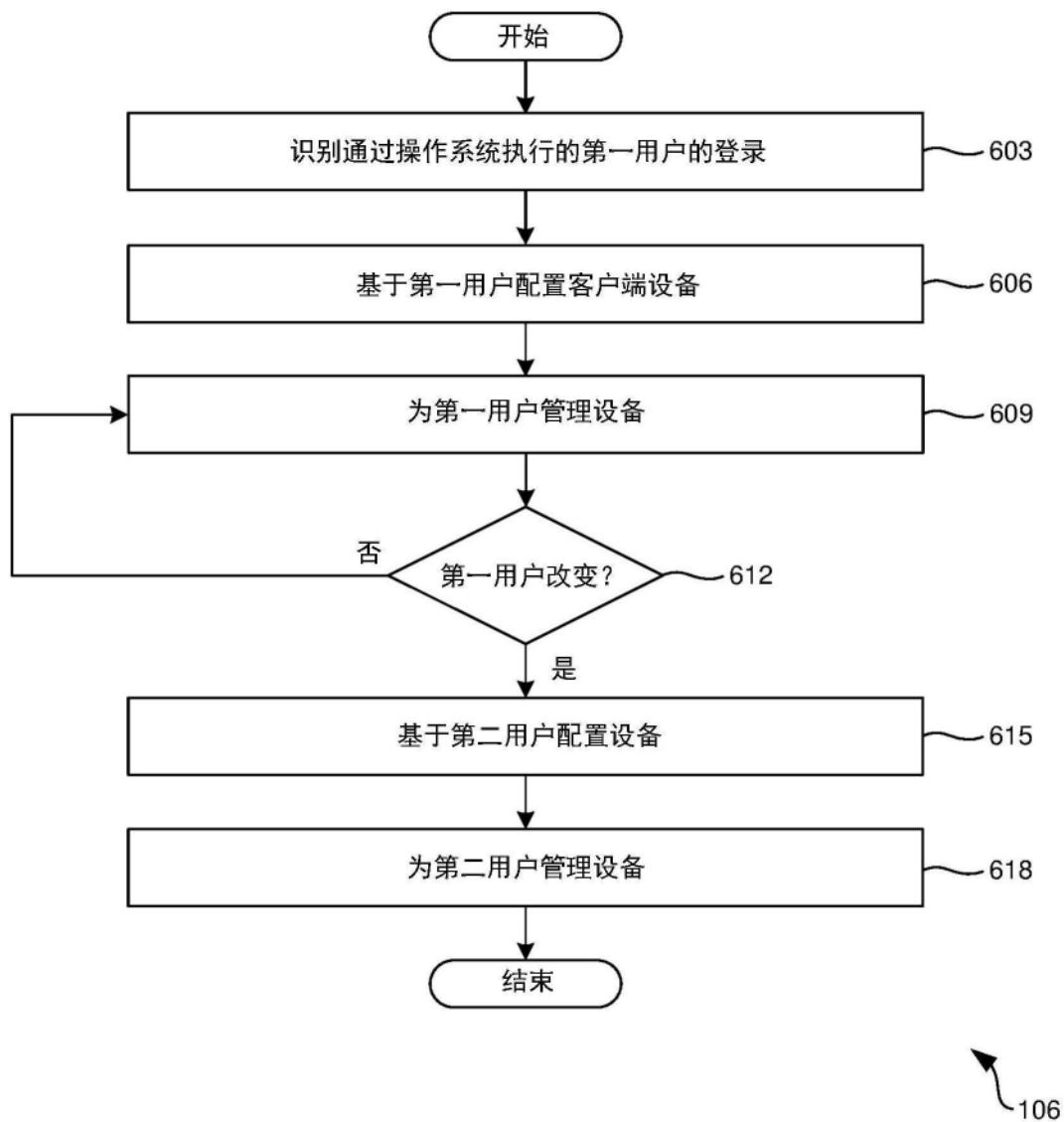


图6