(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118250165 A
(43)申请公布日 2024.06.25

(21)申请号 202410388468.6

(22)申请日 2019.06.19

(30)优先权数据
16/037,201 2018.07.17 US

(62)分案原申请数据
201980047014.X 2019.06.19

(71)申请人 微软技术许可有限责任公司
地址 美国华盛顿州

(72)发明人 S·拉希里 R·I·朱恩
P·J·考夫曼 朱于航

(74)专利代理机构 北京世辉律师事务所 16093
专利代理师 王俊

(51)Int.Cl.
H04L 41/0806(2022.01)
H04L 41/0853(2022.01)
H04L 41/0869(2022.01)
H04L 9/40(2022.01)
H04L 67/00(2022.01)
H04W 12/08(2021.01)
H04W 12/37(2021.01)
G06Q 10/0635(2023.01)

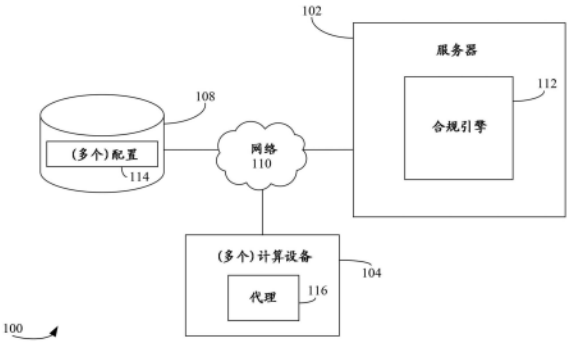
权利要求书2页 说明书15页 附图8页

(54)发明名称

用于移动设备管理的基于无查询设备配置确定的技术

(57)摘要

在本文中所描述的实施例涉及用于移动设备管理的基于无查询设备配置确定的技术,并且具体涉及管理被连接至企业网络的设备的设备合规性。例如,移动设备管理器可以向计算设备提供配置设置,计算设备实现设置以便符合企业的数据策略和/或安全策略。移动设备管理器还维持对每个设备的由此而实现的配置设置的本地引用。当移动设备管理器随后执行关于计算设备是否仍然合规的确定时,移动设备管理器仅需要参照本地引用来确定计算设备的设置,而不是显式地向计算设备查询其设置。前述技术可以针对安全基线合规性确定、IoT设备合规性确定以及对其他类型的设备(诸如由企业的利用企业的网络的商业伙伴利用的设备)的合规性确定而被扩展。



CN 118250165 A

1.一种系统,包括:

处理单元;

存储器,所述存储器耦合到所述处理单元并且包括计算机可执行指令,当所述计算机可执行指令被执行时,执行操作,所述操作包括:

响应于由第一设备检测到的触发事件,访问与用户以及第二设备相关联的第一配置设置;

确定所述第一配置设置不符合与所述第二设备相关联的合规规则;以及

向所述第二设备发送第二配置设置,其中所述第二配置设置使得所述第二设备符合所述合规规则。

2.根据权利要求1所述的系统,其中所述触发事件是以下项中的一项:

预定时间段的到期;

所述第二设备的先前配置设置已经改变的指示;或者

用户已经登录到所述第二设备的指示。

3.根据权利要求1所述的系统,其中所述第一配置设置被存储在所述第一设备的配置引用中,所述配置引用包括多个条目,所述多个条目中的每个条目指定用户-设备配对以及由所述用户-设备配对实现的对应的配置设置。

4.根据权利要求3所述的系统,所述操作还包括:

响应于确定所述第一配置设置不符合所述合规规则,更新存储在所述第一设备中的合规记录以指示所述第二设备合规。

5.根据权利要求4所述的系统,其中当所述第二设备被配置为具有所述第一配置设置时,更新所述合规记录使得所述第二设备先前可访问的一个或多个资源对于所述第二设备变得不可访问。

6.根据权利要求5所述的系统,当所述第二设备被配置为具有所述第二配置设置时,所述一个或多个资源对于所述第二设备是可访问的。

7.根据权利要求3所述的系统,向所述第二设备发送所述第二配置设置包括更新所述配置引用以指示所述第二配置设置当前与所述用户以及所述第二设备相关联。

8.根据权利要求1所述的系统,确定所述第一配置设置不符合所述合规规则包括:

将所述第一配置设置与所述合规规则进行比较;以及

确定所述第一配置设置的一个或多个属性与所述合规规则的一个或多个对应的属性不匹配。

9.根据权利要求1所述的系统,所述操作还包括:

从所述第二设备接收所述第二配置设置已经被应用于所述第二设备的确认;以及

响应于所述确认,将所述第二设备指定为符合所述合规规则。

10.根据权利要求1所述的系统,其中所述第一设备包括:

所述合规规则;以及

合规引擎,所述合规引擎确定所述第一配置设置是否符合所述合规规则。

11.根据权利要求1所述的系统,其中所述第二配置设置指定以下至少一项:

待由所述第二设备实现的加密设置;

待由所述第二设备实现的安全设置;或者

需要被安装在所述第二设备上的应用或者操作系统中的至少一个的最低版本。

12.根据权利要求11所述的系统,其中所述加密设置指定是否要对包括在所述第二设备中的存储设备进行加密。

13.根据权利要求11所述的系统,其中所述安全设置指定以下至少一项:

待由所述第二设备实现的密码策略;

代码签名是否由所述第二设备实现;或者

可信平台模块(TPM)是否由所述第二设备实现。

14.一种方法,包括:

响应于由第一设备检测到的触发事件,访问由第二设备实现的第一配置设置,所述第一配置设置与用户-设备配对相关联,所述用户-设备配对标识用户和所述第二设备;

确定所述第一配置设置不符合与适用于所述第二设备的合规规则,所述合规规则由所述第一设备存储;以及

向所述第二设备发送第二配置设置,其中所述第二配置设置旨在通过替换所述第二设备上的所述第一配置设置以使得所述第二设备符合所述合规规则。

15.根据权利要求14所述的方法,其中所述第一设备包括:

合规引擎,所述合规引擎用于确定配置设置是否符合合规规则;

配置引用,所述配置引用包括所述第一配置设置和所述第二配置设置;以及

合规记录,所述合规记录包括每个存储的用户-设备配对是否合规。

16.根据权利要求14所述的方法,所述合规规则由企业的管理员指定,所述第二设备是所述企业的成员。

17.根据权利要求14所述的方法,所述第一配置设置由第三方计算设备提供。

18.根据权利要求14所述的方法,响应于所述第二配置设置被应用于所述第二设备,接收指示所述第二设备符合所述合规规则的确认。

19.根据权利要求18所述的方法,还包括:

在所述第一设备存储:

所述第二设备被配置具有所述第二配置设置的指示;以及

所述第二设备符合所述合规规则的指示。

20.一种移动设备管理器,包括:

处理单元;

存储器,所述存储器耦合到所述处理单元并且包括计算机可执行指令,当所述计算机可执行指令被执行时,执行操作,所述操作包括:

响应于检测触发事件,访问由所述移动设备管理器存储的配置设置,所述配置设置与移动设备相关;

确定所述配置设置不符合合规规则,所述移动设备受制于所述合规规则;以及

响应于确定所述配置设置不符合所述合规规则,使得企业的资源对于所述移动设备不可访问,所述移动设备是是所述企业的成员。

用于移动设备管理的基于无查询设备配置确定的技术

[0001] 相关申请

[0002] 本申请是申请号为201980047014.X、发明名称为“用于移动设备管理的基于无查询设备配置确定的技术”的发明专利申请的分案申请。

背景技术

[0003] 移动设备管理(MDM)是一种用于确保员工保持生产力并且不违反公司策略的方式。许多组织使用MDM产品/服务来控制其员工的活动。MDM主要应对公司数据分离、保护电子邮件、保护设备上的公司文档、强制执行公司策略以及集成和管理移动设备(包括各种类别的膝上型电脑和手持式设备)。通过控制和保护组织的网络中的所有移动设备的数据和配置设置,MDM可以降低支持成本和商业风险。

发明内容

[0004] 本发明内容被提供以按照简化形式来介绍对构思的选择,这些构思下面在具体实施方式中被进一步描述。本发明内容不旨在标识所要求保护的主题的关键特征或者本质特征,也不旨在被用于限制所要求保护的主题的范围。

[0005] 在本文中所描述的实施例涉及管理针对被连接至网络(例如企业网络)的设备的设备合规性。例如,移动设备管理器可以向计算设备提供配置设置,该计算设备实现设置以便符合企业的策略(例如数据和/或安全策略)。移动设备管理器还维持对每个设备的由此而实现的配置设置的本地引用。当移动设备管理器随后执行关于计算设备是否仍然合规的确定时,移动设备管理器仅需要参照本地引用来确定计算设备的设置,而不是显式地向计算设备查询其设置。前述技术可以针对安全基线合规性确定、物联网(IoT)设备合规性确定以及对其他类型的设备(诸如由企业的利用企业的网络的商业伙伴利用的设备)的合规性确定而被扩展。

[0006] 下面参照附图对本发明的其他特征和优点以及本发明的各种实施例的结构和操作进行了详细描述。应该注意,本发明不限于在本文中所描述的特定实施例。本文仅出于说明性目的而呈现这种实施例。基于本文中所包括的教导,对于(多个)相关领域的技术人员而言,附加实施例将是明显的。

附图说明

[0007] 被并入本文并且形成本说明书的一部分的附图图示了实施例,并且与本说明书一起进一步用于解释实施例的原理以及使相关领域的技术人员能够形成和使用实施例。

[0008] 图1描绘了根据示例实施例的用于管理设备合规性的系统的框图。

[0009] 图2描绘了根据示例实施例的用于管理设备合规性的系统的框图,该系统是图1所示系统的进一步详细示例。

[0010] 图3描绘了根据示例实施例的用于管理设备合规性的示例方法的流程图。

[0011] 图4描绘了根据示例实施例的用于管理设备合规性的系统的框图。

[0012] 图5描绘了根据示例实施例的用于确定计算设备是否依然符合(多个)合规规则的示例方法的流程图。

[0013] 图6描绘了根据实施例的用于确定计算设备是否依然符合(多个)合规规则的系统的框图。

[0014] 图7是其中实施例可以被实现的示例性用户设备的框图。

[0015] 图8是可以被用于实现实施例的示例计算设备的框图。

[0016] 当结合附图时,本发明的特征和优点将通过下面所阐述的详细描述变得更明显,在这些附图中,相同的附图标记始终标识对应的元件。在附图中,附图标记通常指示相同的、在功能上类似的和/或在结构上类似的元件。元件首次出现的附图由对应的附图标记中的(多个)最左边的数字指示。

具体实施方式

[0017] I.介绍

[0018] 本说明书和附图公开了包含本发明的特征的一个或多个实施例。本发明的范围不限于所公开的实施例。所公开的实施例仅例示了本发明,并且所公开的实施例的修改版本也由本发明所涵盖。本发明的实施例由所附权利要求书限定。

[0019] 本说明书中对“一个实施例”、“实施例”、“示例实施例”等的引用指示:所描述的实施例可以包括特定特征、结构或者特性,但是每个实施例可以不一定包括特定特征、结构或者特性。此外,这种短语不一定是指相同的实施例。进一步地,当结合实施例对特定特征、结构或者特性进行描述时,应当认为:结合明确地进行了描述或者未明确地进行描述的其他实施例来实现这种特征、结构或者特性在本领域的技术人员的知识范围内。

[0020] 许多示例性实施例被描述如下。应该注意,在本文中所提供的任何章节标题/子章节标题都不旨在是限制性的。贯穿本文对实施例进行了描述,并且任何类型的实施例可以被包括在任何章节/子章节下。此外,可以按照任何方式来将在任何章节/子章节中所公开的实施例与在相同章节/子章节和/或不同章节/子章节中所描述的任何其他实施例组合。

[0021] II.用于管理设备合规性的系统和方法

[0022] 在本文中所描述的实施例涉及管理被连接至网络(例如企业网络)的设备的设备合规性。例如,在服务器处的移动设备管理器可以向计算设备提供配置设置,该计算设备实现设置以便符合企业的策略(例如数据和/或安全策略)。移动设备管理器还维持对每个设备的由此而实现的配置设置的本地引用。当移动设备管理器随后执行关于计算设备是否仍然合规的确定时,移动设备管理器仅需要参照本地引用来确定计算设备的设置,而不是显式地向计算设备查询其设置。前述技术可以针对安全基线合规性确定、物联网(IoT)设备合规性确定以及对其他类型的设备(诸如由企业的利用企业的网络的商业伙伴利用的设备)的合规性确定而被扩展。

[0023] 前述技术在移动设备管理器与计算设备之间建立信任(即,设备信任),其中设备被期望维持其配置设置,并且如果这种设置被改变,则通知移动设备管理器。因此,本地引用总是反映特定设备的配置设置,从而使得移动设备管理器能够确定设备的配置设置,而无需向设备进行查询。这种技术比向设备查询其设置更可靠,因为查询和由设备提供的对那些查询的响应都容易出错(例如传输错误)。

[0024] 此外,由于合规性检查被执行,而不必向计算设备查询其配置设置,因此,跨企业的网络的网络业务有利地被减少,从而释放了网络带宽。此外,利用这种技术,计算设备的少量计算资源被利用,并且实现了低功耗,因为不再需要计算设备响应来自移动设备管理器的许多配置查询。

[0025] 更进一步地,前述技术提供了对其他技术的改进,即,移动设备管理。即,上面所描述的无查询技术引起更快的合规性检查,因为对配置设置的本地引用被咨询来确定设备的设置,而不是必须等待设备通过网络来响应配置设置查询。

[0026] 图1是根据实施例的用于管理设备合规性的系统100的框图。如在图1中所示出的,系统100包括经由企业网络110被通信地耦合的服务器102、一个或多个计算设备104和一个或多个数据存储库108。(多个)数据存储库108可以包括一个或多个物理存储器和/或(多个)存储设备。(多个)数据存储库108可以是在本文中所描述的和/或如将由受益于本公开的(多个)相关领域的技术人员所理解的任何类型的物理存储器和/或存储设备。企业网络110包括由企业出于以下目的而建立的专用计算机网络:将在一个或多个企业位置处的企业设备(例如(多个)计算设备104)相互连接至其他企业设备,并且使得企业设备能够访问和/或共享计算资源。

[0027] (多个)计算设备104旨在表示由企业的成员(例如员工)利用或者以其他方式由企业的成员(例如员工)可访问的设备。如在本文中所使用的,术语“企业”广泛地指代各种组织类型中的任何组织类型,包括:商业、非营利组织和政府机构。(多个)计算设备104的用户在本文中可以被称为“企业用户”或者简称为“用户”。(多个)计算设备104中的每个计算设备可以包括例如但不限于:台式计算机、膝上型计算机、平板计算机、上网本、智能电话等。下面参照图7和图8对(多个)计算设备104的附加示例进行了描述。

[0028] (多个)数据存储库108被配置为存储用于(多个)计算设备104的一个或多个配置112。(多个)配置114中的每个配置114可以为(多个)计算设备104中的特定计算设备和/或(多个)计算设备104中的每个计算设备的特定用户指定一个或多个配置设置。因此,(多个)计算设备104中的每个计算设备可以与(多个)配置114中的多于一个配置相关联。例如,(多个)配置114中的第一配置可以与特定计算设备的第一用户相关联,并且(多个)配置114中的第二配置可以与特定计算设备的第二用户相关联。配置和配置所对应的特定计算设备的特定用户在本文中被称为用户-设备配对(user-device pair)。配置设置的示例包括但不限于:待由(多个)计算设备104实现的加密设置、待由(多个)计算设备104实现的安全设置、需要被安装在(多个)计算设备104上的应用或者操作系统中的至少一个的最低版本等。(多个)加密设置可以指定计算设备104中所包括的存储设备是否要被加密(例如经由加密程序,诸如但不限于:BitLocker™)。安全设置可以指定待由计算设备104实现的密码策略(例如将密码长度设置为最小10个字符、12个字符等),指定代码签名是否应该由(多个)计算设备104实现,指定可信平台模块(TPM)是否应该由(多个)计算设备104实现等。应该注意,上面所描述的配置设置仅是示例性的,并且可以使用其他配置设置。

[0029] 服务器102可以被配置为相对于由企业指定的策略(例如数据和/或安全策略)管理(多个)计算设备104的合规性。服务器102还可以被称为移动设备管理器。策略可以根据一个或多个合规规则而被指定。例如,服务器102可以包括合规引擎112。合规引擎112可以确定待被提供给(多个)计算设备104中的特定计算设备的(多个)配置114,并且将所确定的

(多个)配置提供给该特定计算设备。所确定的(多个)配置可以符合(多个)合规规则。该(多个)合规规则可以由企业的管理员(例如IT管理员或者企业内可以代表企业用户负责部署、维护和/或配置(多个)计算设备104的其他人员)指定。(多个)计算设备104中的每个计算设备被配置为实现由(多个)配置114指定的(多个)配置设置,并且向服务器102提供确认。该确认指示计算设备已经实现了配置设置。在接收到确认之后,合规引擎112将从其接收到确认的计算设备指定为符合(多个)合规规则。

[0030] 合规引擎112还可以被配置为维持对由(多个)计算设备104中的每个计算设备实现的(多个)配置设置的本地引用。合规引擎112可以被配置为使用引用来确定(多个)计算设备104中的特定计算设备是否依然符合(多个)合规规则。通过这样做,合规引擎112仅需要访问该引用来确定由(多个)计算设备104实现的(多个)配置设置,而不是必须向(多个)计算设备104查询其配置设置。

[0031] 在实施例中,图1所示系统100可以按照各种方式被实现。例如,图2描绘了根据示例实施例的系统200的详细框图。系统200是系统100的示例。如在图2中所示出的,系统200包括服务器202、(多个)计算设备204、(多个)数据存储库208、(多个)第三方计算设备218和(多个)物联网(IoT)设备220,它们中的每一个都经由企业网络210被通信地耦合。服务器202、(多个)计算设备204、(多个)数据存储库208和企业网络210是上面参照图1所分别描述的服务器102、(多个)计算设备104、(多个)数据存储库208和企业网络110的示例。

[0032] (多个)数据存储库208被配置为存储用于多个不同类型的设备的多个不同配置。例如,如在图2中所示出的,(多个)数据存储库208可以存储(多个)设备配置222、(多个)第三方配置228和(多个)原始设备制造方(OEM)配置226。(多个)设备配置222可以指定用于(多个)计算设备204和/或(多个)计算设备204的特定用户的一个或多个配置设置。(多个)OEM配置226可以指定用于(多个)IoT设备220的(多个)配置设置,并且(多个)第三方配置228可以指定用于(多个)第三方计算设备218的(多个)配置设置。(多个)数据存储库208还可以存储(多个)安全基线224,该(多个)安全基线224可以为(多个)设备(诸如(多个)计算设备204、(多个)第三方计算设备218和/或(多个)IoT设备220)指定软件开发人员(例如操作系统(OS)开发人员)为了使(多个)这种设备保持安全而推荐的配置设置。(多个)设备配置222、(多个)第三方配置228、(多个)OEM配置226和(多个)安全基线224中的每一个可以被存储为文件(例如XML文件、文本文件等)。下面对有关(多个)设备配置222、(多个)第三方配置228、(多个)OEM配置226和(多个)安全基线224的附加细节进行了描述。

[0033] (多个)设备配置222可以指定用于(多个)计算设备204的(多个)配置设置,该(多个)计算设备204是由企业维护并且被供应给企业的员工的(多个)计算设备。(多个)设备配置222可以由企业的管理员指定(例如经由图形用户界面(GUI))。(多个)设备配置222根据由服务器202维持的一个或多个合规规则214而被指定。(多个)合规规则214也可以由企业的管理员指定(例如经由GUI)。(多个)合规规则214可以指定以下(多个)配置设置:该(多个)配置设置应该由被连接至企业网络210的(多个)设备(例如(多个)计算设备204、(多个)第三方计算设备218和(多个)IoT设备220)利用以便符合由企业指定的策略。

[0034] 服务器202可以被配置为:确定待被提供给(多个)计算设备204的(多个)设备配置222,并且将所确定的(多个)配置提供给(多个)计算设备204。例如,当用户首次登录到针对其所新配置的计算设备时,服务器202可以获取与该计算设备和/或用户相关联的(多个)设

备配置222,并且将(多个)设备配置222提供给计算设备。如在图2中所示出的,(多个)计算设备204中的每个计算设备可以被配置为执行代理216,该代理216被配置为实现由接收到的设备配置指定的配置设置。在实现设置之后,代理216可以向合规引擎212提供确认。该确认指示计算设备204已经实现了配置设置。在接收到确认之后,合规引擎212将计算设备指定为符合(多个)合规规则214。

[0035] 服务器204可以维持合规记录232,该合规记录232包括针对每个用户-设备配对的关于特定的用户-设备配对是否合规的指定。例如,合规记录232可以包括数据结构(例如表),该数据结构包括多个条目,其中每个条目指定特定的用户-设备配对以及关于该用户-设备配对是否合规的指示。服务器202还可以被配置为维持对针对每个用户-设备配对而实现的配置设置的本地配置引用230。配置引用230可以包括数据结构(例如表),该数据结构包括多个条目,其中每个条目指定特定的用户-设备配对以及由该配对实现的配置设置。应该注意,上面所描述的配置引用230和/或合规记录232的结构和/或组织仅是示例性的,并且可以使用其他结构和/或组织。

[0036] 合规引擎212可以被配置为使用引用230来确定(多个)计算设备204是否依然符合合规规则。通过这样做,合规引擎212仅需要访问引用230来确定由(多个)计算设备204实现的配置设置,而不是必须向(多个)计算设备204查询其配置设置。合规引擎212可以在检测到触发事件之后确定(多个)计算设备204是否依然合规。

[0037] 根据实施例,触发事件是预定时间段的到期。按照这种实施例,合规引擎212可以周期性地将(多个)合规规则214与(多个)计算设备204的配置设置进行比较。随着时间的推移,(多个)合规规则214可以由企业的管理员修改。因此,合规引擎212可以通过使用引用230来周期性地确定由(多个)计算设备204实现的配置设置是否符合(多个)合规规则214。例如,合规引擎212可以使用引用230来查找由(多个)计算设备204利用的(多个)配置设置,并且将(多个)配置设置与(多个)合规规则214进行比较以确定它们是否相符。如果(多个)合规设置不符合(多个)合规规则214,则合规引擎212可以确定(多个)计算设备204不再合规。如果(多个)合规设置确实符合(多个)合规规则214,则合规引擎212可以确定(多个)计算设备204依然合规。

[0038] 根据另一实施例,触发事件是来自(多个)计算设备204的其配置设置已经改变的指示。例如,(多个)计算设备204中的特定计算设备的用户和/或在(多个)计算设备204上执行的应用可以改变配置设置。代理216可以被配置为响应于配置设置被改变而向合规引擎212提供通知。该通知可以指定哪些设置被改变。在从特定计算设备接收到通知之后,合规引擎212确定已改变的设置是否导致特定计算设备不再符合(多个)合规规则214。例如,合规引擎212可以将在通知中所指示的(多个)配置设置与(多个)合规规则214进行比较以确定已改变的设置是否与之相符。如果(多个)配置设置符合(多个)合规规则214,则合规引擎212可以确定特定计算设备依然合规。

[0039] 如果(多个)配置设置不符合(多个)合规规则214,则合规引擎212可以确定特定计算设备不再合规,并且在合规记录232中更新针对计算设备的指定以指示计算设备不再合规。合规引擎212还可以阻止(多个)这种计算设备访问经由企业网络210可访问的资源。这种资源包括但不限于:电子邮件服务器、数据储存库、应用服务器等。对这种资源的访问可以被阻止,直到(多个)计算设备204符合(多个)合规规则214为止。例如,合规引擎212可以

传输符合(多个)合规规则214的新配置设置。在实现(多个)新配置设置之后,代理216可以向合规引擎212传输确认。在接收到确认之后,合规引擎212可以将(多个)计算设备204指定为合规,并且相应地更新合规记录232。

[0040] 根据实施例,代理216被配置为维持由服务器202提供的配置设置。例如,在用户或者在(多个)计算设备上执行的应用尝试改变配置设置的事件中,代理216可以阻止改变发生和/或使改变回滚。在代理216不能阻止配置设置和/或使配置设置回滚的事件中,代理216可以将指示已改变的(多个)设置的通知发送给合规引擎212。

[0041] 根据另一实施例,触发事件是用户已经经由计算设备(例如(多个)计算设备204)登录到企业网络210的指示。例如,计算设备可以被配置为响应于用户登录到计算设备而向服务器202提供通知。在接收到通知之后,合规引擎212可以使用引用230来为已登录用户(即,为用户-设备配对)查找由(多个)计算设备204利用的(多个)配置设置,并且将(多个)配置设置与(多个)合规规则214进行比较以确定它们是否相符。如果(多个)合规设置不符合(多个)合规规则214,则合规引擎212可以确定(多个)计算设备204不再合规。如果(多个)合规设置确实符合(多个)合规规则214,则合规引擎212可以确定(多个)计算设备204依然合规。前述内容使合规引擎212能够对用户-设备配对强制执行合规性,而不必每当用户登录到特定设备时总是向下推送(多个)配置设置。这确保了当基于每个用户对合规性进行评估时,在多用户环境中的合规性可以是立即的。例如,当不同的用户登录到设备时,合规引擎212可以通过访问由服务器202存储的对配置设置的引用230来简单地确定已经针对该用户-设备配对而实现的(多个)配置设置,并且确定已经由设备实现的配置设置与(多个)合规规则214之间是否存在任何差异。如果没有差异,则在合规记录232中,设备立即被指定为合规。前述内容在无需服务器202重新向设备查询其当前的(多个)配置设置的情况下被实现。相比之下,现有技术需要服务器每当用户登录时将用户特定的设置向下推送到设备,并且随后向设备查询其设置。然后,在将从设备接收到的设置与(多个)合规规则进行比较之后,服务器会不得不将设备指定为合规。如果已经由设备实现的现有设置符合(多个)合规规则214,则前述技术完全消除了这种来回通信。

[0042] 如果有差异,则合规引擎212可以为(多个)这种计算设备204更新在合规记录232中的指定以指示(多个)这种设备不再合规。合规引擎212还可以阻止(多个)这种计算设备204访问经由企业网络210可访问的资源。这种资源包括但不限于:电子邮件服务器、数据储存库、应用服务器等。对这种资源的访问可以被阻止,直到(多个)计算设备204符合(多个)合规规则214为止。例如,合规引擎212可以传输符合(多个)合规规则214的新配置设置。在实现了(多个)新配置设置之后,代理216可以向合规引擎212传输确认。在接收到确认之后,合规引擎212可以通过相应地更新合规记录232来将(多个)计算设备204指定为合规。

[0043] 前述内容有利地使合规引擎212能够在从(多个)计算设备204接收到确认之后确定合规性,而不是必须重新向设备查询其设置。这有利地阻止了不合规的用户临时具有网络资源的访问权限。在现有技术中,当服务器向计算设备查询其配置设置并且将设置与合规规则进行比较时,用户将仍然具有网络资源的访问权限。在本文中所公开的技术通过在从代理216接收到确认之后立即检查合规性来阻止这一点。此外,当合规的用户登录到由不同的不合规的用户使用的设备时,这些技术改善了用户体验。在现有技术中,当合规的用户登录到设备时,设备将被标记为不合规,同时服务器向设备查询其配置设置。在本文中所公

开的技术通过在新用户登录到设备之后立即使用引用230检查合规性来消除该问题。

[0044] 根据又一实施例,触发事件是(多个)合规规则214已经改变的指示。例如,当管理员对(多个)合规规则214进行改变时,合规引擎212可以接收表明改变的指示。在接收到指示之后,合规引擎212可以使用引用230来查找由(多个)计算设备204利用的(多个)配置设置,并且将(多个)配置设置与(多个)合规规则214进行比较以确定它们是否合规。如果(多个)配置设置符合(多个)合规规则214,则合规引擎212可以确定特定计算设备依然合规。

[0045] 如果(多个)配置设置不符合(多个)合规规则214,则合规引擎212可以确定特定计算设备不再合规,并且在合规记录232中更新针对计算设备的指定以指示计算设备不再合规。合规引擎212还可以阻止(多个)这种计算设备访问经由企业网络210可访问的资源,直到(多个)这种计算设备变为合规为止。

[0046] (多个)安全基线224可以由操作系统(OS)开发人员周期性地公布和发布作为每个OS版本的一部分,并且是针对许多企业的合规标准的一部分。在常规的场景中,企业需要重新向计算设备进行查询,并且通过每次OS更新来针对其组织中的所有用户-设备配对重新对合规性进行评估。对于企业而言,这是非常昂贵的过程,并且阻碍更快地采用OS。为了克服这种问题,当针对新的OS更新而发布(多个)新的安全基线224时,合规引擎212可以针对新的OS版本/更新向(多个)数据存储库208查询(多个)安全基线224(或者使用其自己的企业特定基线),并且对新的OS版本/更新是否已经使设备上的用户保持合规进行评估。例如,合规引擎212可以使用引用230来查找由每个用户-设备配对利用的(多个)配置设置,并且将(多个)配置设置与(多个)安全基线224进行比较以确定它们是否相符。如果(多个)配置设置不符合(多个)安全基线224,则合规引擎212确定用户-设备配对不合规。作为响应,合规引擎212可以将用户-设备配对指定为不合规,阻止对(多个)企业资源的访问,和/或将更新过的(多个)配置设置提供给相关联的计算设备。如果(多个)配置设置确实符合(多个)安全基线224,则合规引擎212确定用户-设备配对合规。前述技术允许在不需要每个用户登录到特定设备的情况下立即对合规性进行评估。

[0047] (多个)IoT设备220可以默认被分类为安全的,并且具有由这种设备的制造方(也被称为OEM)配置的默认配置。(多个)IoT设备220的示例包括但不限于:视频会议系统、打印机、扬声器、供暖设备、通风和空调(HVAC)系统等。用于这种设备的配置可以被存储在(多个)数据存储库208中(被示出为(多个)OEM配置226)。(多个)IoT设备220的配置设置通常不由最终用户可修改和/或仅由OEM可修改(例如经由软件和/或硬件更新)。为了确定(多个)IoT设备220是否合规,合规引擎212可以向(多个)数据存储库208查询(多个)OEM配置226,并且将用于由企业利用的(多个)IoT设备220中的每个IoT设备220的(多个)OEM配置226与(多个)合规规则214进行比较以确定它们是否相符。如果(多个)IoT设备220不合规,则组织可以通知制造方更新(多个)这种设备的配置设置,使得它们合规。如果(多个)IoT设备220符合(多个)合规规则,则合规引擎212可以在合规记录232中将(多个)这种设备指定为合规。

[0048] 在OEM经由更新来改变设备的配置设置的事件中,OEM可以将更新过的(多个)OEM配置226提供给企业,并且合规引擎212可以重新对合规性进行评估。这有利地使合规引擎212能够使用(多个)OEM配置226来对(多个)IoT设备220进行批处理,而不是必须通过单独地向每个IoT设备220查询其配置来对(多个)IoT设备220中的每个IoT设备进行评估。

[0049] 配置设置还可以由第三方实体提供。例如,如在图2中所示出的,(多个)第三方配置228指定用于(多个)第三方计算设备218的配置设置,该(多个)第三方计算设备218可以是与企业的商业伙伴相关联的(多个)设备。例如,这种伙伴的员工可以出于商业目的而拜访企业。可以使用(多个)第三方配置228来针对合规性而检查(多个)第三方计算设备218。第三方可以在第三方的员工到达企业的站点之前将(多个)第三方配置228提供给企业,并且在到达之前,合规引擎212可以确定(多个)第三方计算设备218是否符合(多个)合规规则214。如果(多个)第三方计算设备218不合规,则企业可以通知第三方需要对其设备的配置进行改变,并且向他们告知所需的配置设置。第三方可以相应地更新配置设置,并且将更新过的(多个)第三方配置228提供给企业。然后,合规引擎218可以使用更新过的(多个)第三方配置228来重新对合规性进行评估,并且向第三方通知(多个)第三方计算设备218现在是否合规。这有利地使得在到达之后,(多个)第三方计算设备218能够立即具有企业网络210及其资源的访问权限,而不是必须在(多个)第三方计算设备218连接至企业网络210之后等待企业管理其设备并且对合规性进行评估。

[0050] 因此,可以按照许多方式来针对合规性对设备进行管理。例如,图3描绘了根据示例实施例的由服务器实现的、用于管理设备合规性的示例方法的流程图300。现在将参照图4所示系统400来对流程图300的方法进行描述,但是该方法不限于该实现。图4是根据另一实施例的用于管理设备合规性的系统400的框图。如在图4中所示出的,系统400包括服务器402、一个或多个计算设备404和一个或多个数据存储库408。服务器402、(多个)计算设备404和(多个)数据存储库408经由企业网络410被通信地耦合。服务器402、(多个)计算设备404、(多个)数据存储库408和企业网络410是如上面参照图2所描述的服务器202、(多个)计算设备204、(多个)数据存储库208和企业网络210的示例。如在图4中所进一步示出的,服务器402包括合规引擎412、一个或多个合规规则414、配置引用430和合规记录432。(多个)计算设备404分别包括代理416,并且(多个)数据存储库408包括(多个)配置420。合规引擎412、(多个)合规规则414、(多个)配置引用430、合规记录432和代理416是如上面参照图2所分别描述的合规引擎212、(多个)合规规则214、配置引用230、合规记录232和代理216的示例。(多个)配置420是如上面参照图2所描述的(多个)设备配置222、(多个)安全基线224、(多个)OEM配置226和/或(多个)第三方配置228的示例。基于有关流程图300和图4所示系统400的讨论,对于(多个)相关领域的技术人员而言,其他结构实施例和操作实施例将是明显的。

[0051] 如在图3中所示出的,流程图300的方法从步骤302开始,在该步骤302中,用于计算设备的配置设置被确定,该计算设备经由通信地耦合服务器和计算设备的网络可访问。例如,参照图4,服务器402确定用于经由企业网络410可访问的(多个)计算设备404的配置设置。

[0052] 根据一个或多个实施例,配置设置指定以下至少一项:待由计算设备实现的加密设置、待由计算设备实现的安全设置或者需要被安装在计算设备上的应用或者操作系统中的至少一个的最低版本。

[0053] 根据一个或多个实施例,通过标识已经登录到计算设备的用户并且确定与用户和计算设备相关联的配置设置来对用于计算设备的配置设置进行确定。例如,企业的管理员可以为(多个)计算设备404中的每个计算设备和/或为(多个)计算设备404中的特定计算设

备的每个用户不同地对配置设置进行配置。管理员可以确保这种设置符合与之相关联的(多个)合规规则414。这种配置设置可以作为(多个)配置420被存储在(多个)数据存储库408中。当用户首次登录到向其新供应的计算设备时,服务器402可以从与该计算设备和用户(即,用户-设备配对)相关联的(多个)数据存储库408确定配置,并且获取该配置(被示出为配置401)。

[0054] 在步骤304中,配置设置经由网络被传输给计算设备。例如,参照图4,服务器402经由网络410来将配置401传输给(多个)计算设备404。

[0055] 在步骤306中,在服务器上维持对配置设置的引用。例如,参照图4,服务器402维持对被传输给(多个)计算设备404的配置(即,配置401)的本地配置引用430。引用430可以包括对被提供给特定的用户-设备配对的(多个)配置设置进行映射的数据结构(例如表)。例如,数据结构可以指定哪个(哪些)配置设置已经被提供并且待由特定的用户-设备配对实现。

[0056] 在步骤308中,经由网络来从计算设备接收配置设置已经被实现的确认。例如,参照图4,代理416经由企业网络410来将确认403发送给服务器402。确认403指示代理416已经在(多个)计算设备404上实现了由配置401指定的配置设置。

[0057] 在步骤310中,响应于接收到确认而将计算设备指定为符合合规规则。例如,参照图4,合规引擎412可以更新与(多个)计算设备404相对应的条目合规记录432以指示(多个)计算设备404投诉。

[0058] 图5描绘了根据示例实施例的用于确定计算设备是否依然符合(多个)合规规则的示例方法的流程图500。现在将参照图6所示系统600来对流程图500的方法进行描述,但是该方法不限于该实现。图6是根据实施例的用于确定计算设备是否依然符合(多个)合规规则的系统600的框图。如在图6中所示出的,系统600包括服务器602、一个或多个计算设备604和一个或多个数据存储库608。服务器602、(多个)计算设备604和(多个)数据存储库608经由企业网络610被通信地耦合。服务器602、(多个)计算设备604、(多个)数据存储库608和企业网络610是如上面参照图4所描述的服务器402、(多个)计算设备404、(多个)数据存储库408和企业网络410的示例。如在图6中所进一步示出的,服务器602包括合规引擎612、一个或多个合规规则614、配置引用630和合规记录632。(多个)计算设备604包括代理616,并且(多个)数据存储库608包括(多个)配置620。合规引擎612、(多个)合规规则614、配置引用630和合规记录632以及代理616是如上面参照图4所分别描述的合规引擎412、(多个)合规规则414、配置引用430和合规记录432以及代理416的示例。(多个)配置620是如上面参照图4所描述的(多个)配置420的示例。基于有关流程图500和图6所示系统600的讨论,对于(多个)相关领域的技术人员而言,其他结构实施例和操作实施例将是明显的。

[0059] 如在图5中所示出的,流程图500的方法从步骤502开始,在该步骤502中,通过响应于检测到触发事件将对配置设置的引用与合规规则进行比较来关于计算设备是否依然符合合规规则进行确定。例如,参照图6,合规引擎612通过响应于检测到触发事件将配置引用230与(多个)合规规则214进行比较来确定(多个)计算设备604是否依然符合(多个)合规规则614。响应于确定计算设备不再合规,流程继续至步骤504。否则,流程继续至步骤506。

[0060] 根据一个或多个实施例,触发事件包括以下至少一项:预定时间段的到期;从计算设备接收到的、计算设备的第二配置设置已经改变的指示;或者用户已经登录到计算设备

的指示。例如,参照图6,合规引擎612可以维持定时器,该定时器在到期时使合规引擎612将(多个)计算设备604的(多个)配置设置(如由(多个)配置引用606指示的)与(多个)合规规则614进行比较。在另一实施例中,代理616可以经由网络610来将指示(多个)计算设备604的第二配置设置已经改变的指示601提供给合规引擎612。在另一示例中,(多个)计算设备604中的特定计算设备可以经由企业网络610来向服务器602提供用户已经登录到网络610和/或计算设备的指示603。

[0061] 在步骤504中,计算设备被阻止访问经由网络可访问的资源,并且计算设备被指定为不符合合规规则。例如,参照图6,合规引擎612阻止(多个)计算设备604访问经由企业网络610可访问的资源,并且将(多个)计算设备604指定为不符合(多个)合规规则614。例如,合规引擎612可以向(多个)计算设备604传输禁止对企业网络610资源的访问的命令607。合规引擎612还更新与(多个)计算设备604相对应的合规记录632中的条目,以指示(多个)计算设备604不再合规。

[0062] 根据一个或多个实施例,响应于确定计算设备不再合规,经由网络来将符合合规规则的新配置设置传输给计算设备。例如,参照图6,管理员可以更新(多个)配置420,使得它们符合(多个)合规规则414。合规引擎612可以获取更新过的(多个)配置和/或经由企业网络610来将更新过的(多个)配置(被示出为配置405)传输给代理616,该代理616实现由此而指定的新配置设置。

[0063] 在步骤506中,维持计算设备合规的指定。例如,参照图6,合规引擎612在合规记录632中维持(多个)计算设备604符合(多个)合规规则614的指定。

[0064] III.示例移动设备实施例和示例静止设备实施例

[0065] 上面所描述的系统和方法(包括参照图1至图6所描述的设备合规性管理实施例)可以被实现在硬件或者与软件和/或固件中的一者或两者结合的硬件中。例如,合规引擎112、代理116、合规引擎212、(多个)合规规则214、配置引用230、合规记录232、代理216、合规引擎412、(多个)合规规则414、配置引用430、合规记录432、代理416和/或在其中以及流程图300和/或流程图500中所描述的组件中的每个组件分别被实现为被配置为在一个或多个处理器中被执行并且被存储在计算机可读存储介质中的计算机程序代码/指令。备选地,合规引擎112、代理116、合规引擎212、(多个)合规规则214、配置引用230、合规记录232、代理216、合规引擎412、(多个)合规规则414、配置引用430、合规记录432、代理416和/或在其中以及流程图300和/或流程图500中所描述的组件中的每个组件可以被实现为硬件逻辑/电气电路装置。在实施例中,合规引擎112、代理116、合规引擎212、(多个)合规规则214、配置引用230、合规记录232、代理216、合规引擎412、(多个)合规规则414、配置引用430、合规记录432、代理416和/或在其中以及流程图300和/或流程图500中所描述的组件中的每个组件可以被实现在一个或多个SoC(片上系统)中。SoC可以包括集成电路芯片,该集成电路芯片包括以下一项或多项:处理器(例如中央处理单元(CPU)、微控制器、微处理器、数字信号处理器(DSP)等)、存储器、一个或多个通信接口和/或其他电路,并且可以可选地执行接收到的程序代码和/或包括嵌入式固件以执行功能。

[0066] 图7示出了包括总体上被示出为组件702的各种可选的硬件组件和软件组件的示例性移动设备700的框图。如将为(多个)相关领域的技术人员所知的,(多个)计算设备104、(多个)计算设备204、(多个)第三方计算设备218、(多个)IoT设备220、(多个)计算设备404、

(多个)计算设备604、服务器102、服务器402、服务器602、合规引擎112、代理116、合规引擎212、(多个)合规规则214、配置引用230、合规记录232、代理216、合规引擎412、(多个)合规规则414、配置引用430、合规记录432、代理416和/或在其中以及流程图300和/或流程图500中所描述的组件中的每个组件的特征/元素的任何数量和组合可以被实现为移动设备实施例中所包括的组件702以及附加的和/或备选的特征/元素。应该注意,任何组件702都可以与任何其他组件702通信,但是为了便于说明,并非所有连接都被示出。移动设备700可以是在本文中的别处所描述或者提及的或者以其他方式而已知的各种移动设备中的任何移动设备(例如手机、智能电话、手持式计算机、个人数字助理(PDA)等),并且可以允许通过一个或多个通信网络704(诸如蜂窝或者卫星网络)或者利用局域网或者广域网来与一个或多个移动设备的无线双向通信。

[0067] 所图示的移动设备700可以包括控制器或者被称为处理器电路710的处理器以便执行诸如信号编码、图像处理、数据处理、输入/输出处理、功率控制和/或其他功能等任务。处理器电路710是被实现在一个或多个物理硬件电气电路设备元件和/或集成电路设备(半导体材料芯片或者裸片)中作为中央处理单元(CPU)、微控制器、微处理器和/或其他物理硬件处理器电路的电气和/或光学电路。处理器电路710可以执行被存储在计算机可读介质中的程序代码,诸如一个或多个应用714的程序代码、操作系统712、被存储在存储器720中的任何程序代码等。操作系统712可以控制对组件702的分配和使用以及对一个或多个应用程序714(又名应用、“app”等)的支持。应用程序714可以包括常见的移动计算应用(例如电子邮件应用、日历、联系人管理器、web浏览器、消息传递应用)和任何其他计算应用(例如文字处理应用、地图绘制应用、媒体播放器应用)。

[0068] 如图所示,移动设备700可以包括存储器720。存储器720可以包括不可移除存储器722和/或可移除存储器724。不可移除存储器722可以包括RAM、ROM、闪速存储器、硬盘或者其他众所周知的存储器存储技术。可移除存储器724可以包括在GSM通信系统中众所周知的闪速存储器或者订户身份模块(SIM)卡或者其他众所周知的存储器存储技术,诸如“智能卡”。存储器720可以被用于存储用于运行操作系统712和应用714的数据和/或代码。示例数据可以包括待经由一个或多个有线或者无线网络被发送给一个或多个网络服务器或者其他设备和/或从一个或多个网络服务器或者其他设备接收的网页、文本、图像、声音文件、视频数据或者其他数据集。存储器720可以被用于存储订户标识符(诸如国际移动订户身份(IMSI))和设备标识符(诸如国际移动设备标识符(IMEI))。这种标识符可以被传输给网络服务器以标识用户和设备。

[0069] 若干程序可以被存储在存储器720中。这些程序包括操作系统712、一个或多个应用程序714以及其他程序模块和程序数据。这种应用程序或者程序模块的示例可以包括例如用于实现上面所描述的系统(包括参照图1至图6所描述的设备合规性管理实施例)的计算机程序逻辑(例如计算机程序代码或者指令)。

[0070] 移动设备700可以支持一个或多个输入设备730(诸如触摸屏732、麦克风734、相机736、物理键盘738和/或轨迹球740)和一个或多个输出设备750(诸如扬声器752和显示器754)。

[0071] 其他可能的输出设备(未示出)可以包括压电输出设备或者其他触觉输出设备。一些设备可以服务多于一个输入/输出功能。例如,触摸屏幕732和显示器754可以被组合在单

个输入/输出设备中。输入设备730可以包括自然用户界面(NUI)。

[0072] 如本领域中所充分理解的,(多个)无线调制解调器760可以被耦合至(多根)天线(未示出),并且可以支持处理器电路710与外部设备之间的双向通信。(多个)调制解调器760被一般地示出,并且可以包括用于与移动通信网络704和/或其他基于无线电的调制解调器(例如蓝牙764和/或Wi-Fi 762)通信的蜂窝调制解调器766。蜂窝调制解调器766可以被配置为根据任何合适的通信标准或者技术(诸如GSM、3G、4G、5G等)来启用电话呼叫(以及可选地,传输数据)。(多个)无线调制解调器760中的至少一个无线调制解调器760通常被配置用于与一个或多个蜂窝网络(诸如用于在单个蜂窝网络内、蜂窝网络之间或者移动设备与公共交换电话网络(PSTN)之间的数据和语音通信的GSM网络)的通信。

[0073] 移动设备700还可以包括至少一个输入/输出端口780、电源782、卫星导航系统接收器784(诸如全球定位系统(GPS)接收器)、加速度计786和/或物理连接器790,该物理连接器790可以是USB端口、IEEE 1394(火线)端口和/或RS-232端口。如将由本领域的技术人员认识到的,所图示的组件702不被需要或者不是详尽的,因为可以不存在任何组件,并且附加地,可以存在其他组件。

[0074] 此外,图8描绘了其中实施例可以被实现的计算设备800的示例性实现,包括:(多个)计算设备104、(多个)计算设备204、(多个)第三方计算设备218、(多个)IoT设备220、(多个)计算设备404、(多个)计算设备604、服务器102、服务器402、服务器602、合规引擎112、代理116、合规引擎212、(多个)合规规则214、配置引用230、合规记录232、代理216、合规引擎412、(多个)合规规则414、配置引用430、合规记录432、代理416和/或在其中以及流程图300和/或流程图500中所描述的组件中的每个组件。对计算设备800的描述出于说明之目的而被提供,并且不旨在是限制性的。如将为(多个)相关领域的技术人员所知的,实施例可以被实现在其他类型的计算机系统中。

[0075] 如在图8中所示出的,计算设备800包括被称为处理器电路802的一个或多个处理器、系统存储器804和将包括系统存储器804的各种系统组件耦合至处理器电路802的总线806。处理器电路802是被实现在一个或多个物理硬件电气电路设备元件和/或集成电路设备(半导体材料芯片或者裸片)中作为中央处理单元(CPU)、微控制器、微处理器和/或其他物理硬件处理器电路的电气电路和/或光学电路。处理器电路802可以执行被存储在计算机可读介质中的程序代码,诸如操作系统830的程序代码、应用程序832、其他程序834等。总线806表示若干类型的总线结构中的任何一种或多种总线结构,包括:使用各种总线架构中的任何总线架构的存储器总线或者存储器控制器、外围总线、加速图形端口以及处理器或者本地总线。系统存储器804包括只读存储器(ROM)808和随机存取存储器(RAM)810。基本输入/输出系统812(BIOS)被存储在ROM 808中。

[0076] 计算设备800还具有以下设备中的一个或多个设备:用于从硬盘进行读取和写入硬盘的硬盘驱动器814、用于从可移除磁盘818进行读取或者写入可移除磁盘818的磁盘驱动器816、以及用于从可移除光盘822(诸如CD ROM、DVD ROM或者其他光学介质)进行读取或者写入可移除光盘822的光盘驱动器820。硬盘驱动器814、磁盘驱动器816和光盘驱动器820分别通过硬盘驱动器接口824、磁盘驱动器接口826和光学驱动器接口828被连接至总线806。驱动器及其相关联的计算机可读存储介质为计算机提供对计算机可读指令、数据结构、程序模块和其他数据的非易失性存储。虽然对硬盘、可移除磁盘和可移除光盘进行了描

述,但是其他类型的基于硬件的计算机可读存储介质可以被用于存储数据,诸如闪存卡、数字视频磁盘、RAM、ROM和其他硬件存储介质。

[0077] 多个程序模块可以被存储在硬盘、磁盘、光盘、ROM或者RAM上。这些程序包括操作系统830、一个或多个应用832、其他程序834和程序数据836。应用程序832或者其他程序834可以包括例如用于实现上面所描述的系统(包括参照图1至图6所描述的设备合规性管理实施例)的计算机程序逻辑(例如计算机程序代码或者指令)。

[0078] 用户可以通过输入设备(诸如键盘838和指向设备840)来将命令和信息输入到计算设备800中。其他输入设备(未示出)可以包括麦克风、操纵杆、游戏手柄、碟形卫星天线、扫描仪、触摸屏和/或触摸板、用于接收语音输入的语音识别系统、用于接收手势输入的手势识别系统等。这些以及其他输入设备通常通过被耦合至总线806的串行端口接口842被连接至处理器电路802,但是可以通过其他接口被连接,诸如并行端口、游戏端口或者通用串行总线(USB)。

[0079] 显示屏幕844也经由接口(诸如视频适配器846)被连接至总线806。显示屏幕844可以在计算设备800的外部,或者被并入计算设备800。显示屏幕844可以显示信息,以及是用于接收用户命令和/或其他信息(例如通过触摸、手指手势、虚拟键盘等)的用户界面。除了显示屏幕844之外,计算设备800还可以包括其他外围输出设备(未示出),诸如扬声器和打印机。

[0080] 计算设备800通过适配器或者网络接口850、调制解调器852或者用于通过网络来建立通信的其他装置被连接至网络848(例如互联网)。如在图8中所示出的,可以在内部或者在外部的调制解调器852可以经由串行端口接口842被连接至总线806,或者可以使用包括并行接口的另一接口类型被连接至总线806。

[0081] 如在本文中所使用的,术语“计算机程序介质”、“计算机可读介质”和“计算机可读存储介质”通常被用于指代诸如与硬盘驱动器814相关联的硬盘、可移除磁盘818、可移除光盘822等物理硬件介质;诸如RAM、ROM、闪存卡、数字视频磁盘、zip磁盘、MEM、基于纳米技术的存储设备等其他物理硬件介质;以及其他类型的物理/有形硬件存储介质(包括图8所示系统存储器804)。这种计算机可读存储介质区别于通信介质并且不与通信介质重叠(不包括通信介质)。通信介质通常在已调制的数据信号(诸如载波)中实施计算机可读指令、数据结构、程序模块或者其他数据。术语“已调制的数据信号”是指具有按照对信号中的信息进行编码的方式被设置或者改变的其特性中的一个或多个特性的信号。通过示例的方式而非限制,通信介质包括无线介质(诸如声学无线介质、RF、红外无线介质和其他无线介质)以及有线介质。实施例也涉及这种通信介质。

[0082] 如上面所提到的,计算机程序和模块(包括应用程序832和其他程序834)可以被存储在硬盘、磁盘、光盘、ROM、RAM或者其他硬件存储介质上。这种计算机程序还可以经由网络接口850、串行端口接口852或者任何其他接口类型被接收。这种计算机程序在由应用执行或者加载时使计算设备800能够实现在本文中所讨论的实施例的特征。因此,这种计算机程序表示计算设备800的控制器。

[0083] 实施例还涉及包括被存储在任何计算机可读介质上的计算机代码或者指令的计算机程序产品。这种计算机程序产品包括硬盘驱动器、光盘驱动器、存储器设备包、便携式记忆棒、存储卡和其他类型的物理存储硬件。

[0084] IV.附加示例性实施例

[0085] 本文对一种由服务器实现的方法进行了描述。该方法包括:确定用于计算设备的配置设置,该计算设备经由通信地耦合服务器和计算设备的网络可访问;经由网络来将配置设置传输给计算设备;在服务器上维持对配置设置的引用;经由网络来从计算设备接收配置设置由此已经被实现的确认;以及响应于接收到确认而将计算设备指定为符合合规性。

[0086] 在该方法的实施例中,该方法还包括:通过响应于检测到触发事件而将对配置设置的引用与合规规则进行比较,来确定计算设备是否依然符合合规规则;响应于确定计算设备不再合规,阻止计算设备访问经由网络可访问的资源并且指定计算设备不符合合规规则;以及响应于确定计算设备依然合规,维持计算设备合规的指定。

[0087] 在该方法的实施例中,资源包括以下至少一项:经由网络可访问的电子邮件服务器;经由网络可访问的数据储存库;或者经由网络可访问的应用服务器。

[0088] 在该方法的实施例中,该方法还包括:响应于确定计算设备不再合规,经由网络来将符合合规规则的新配置设置传输给计算设备。

[0089] 在该方法的实施例中,触发事件包括以下至少一项:预定时间段的到期;从计算设备接收到的、计算设备的第二配置设置已经改变的指示;或者用户已经登录到计算设备的指示。

[0090] 在该方法的实施例中,配置设置指定以下至少一项:待由计算设备实现的加密设置;待由计算设备实现的安全设置;或者需要被安装在计算设备上的应用或者操作系统中的至少一个的最低版本。

[0091] 在该方法的实施例中,确定用于计算设备的配置设置包括:标识已经登录到计算设备的用户;以及确定与用户和计算设备相关联的配置设置。

[0092] 本文对一种服务器进行了描述。该服务器包括:至少一个处理器电路,以及至少一个存储器,存储被配置为待由至少一个处理器电路执行的程序代码,程序代码包括:合规引擎,被配置为:确定用于计算设备的配置设置,计算设备经由通信地耦合服务器和计算设备的网络可访问;经由网络来将配置设置传输给计算设备;在服务器上维持对配置设置的引用;经由网络来从计算设备接收配置设置由此已经被实现的确认;以及响应于接收到确认而将计算设备指定为符合合规规则。

[0093] 在该服务器的实施例中,合规引擎还被配置为:通过响应于检测到触发事件而将对配置设置的引用与合规规则进行比较,来确定计算设备是否依然符合合规规则;响应于确定计算设备不再合规,阻止计算设备访问经由网络可访问的资源并且指定计算设备不符合合规规则;以及响应于确定计算设备依然合规,维持计算设备合规的指定。

[0094] 在该服务器的实施例中,资源包括以下至少一项:经由网络可访问的电子邮件服务器;经由网络可访问的数据储存库;或者经由网络可访问的应用服务器。

[0095] 在该服务器的实施例中,合规引擎还被配置为:响应于确定计算设备不再合规,经由网络来将符合合规规则的新配置设置传输给计算设备。

[0096] 在该服务器的实施例中,触发事件包括以下至少一项:预定时间段的到期;从计算设备接收到的、计算设备的第二配置设置已经改变的指示;或者用户已经登录到计算设备的指示。

[0097] 在该服务器的实施例中,配置设置指定以下至少一项:待由计算设备实现的加密设置;待由计算设备实现的安全设置;或者需要被安装在计算设备上的应用或者操作系统中的至少一个的最低版本。

[0098] 根据该服务器的实施例中,合规引擎还被配置为确定用于计算设备的配置设置,包括:标识已经登录到计算设备的用户;以及确定与用户和计算设备相关联的配置设置。

[0099] 一种其上记录有程序指令的计算机可读存储介质,这些程序指令在由至少一个处理器执行时执行一种方法,在本文中对该方法进行了进一步描述。该方法包括:确定用于计算设备的配置设置,计算设备经由通信地耦合服务器和计算设备的网络可访问;经由网络来将配置设置传输给计算设备;在服务器上维持对配置设置的引用;经由网络来从计算设备接收配置设置由此已经被实现的确认;以及响应于接收到确认而将计算设备指定为符合合规规则。

[0100] 在该计算机可读存储介质的实施例中,该方法还包括:通过响应于检测到触发事件而将对配置设置的引用与合规规则进行比较,来确定计算设备是否依然符合合规规则;响应于确定计算设备不再合规,阻止计算设备访问经由网络可访问的资源并且指定计算设备不符合所述合规规则;以及响应于确定计算设备依然合规,维持计算设备合规的指定。

[0101] 在该计算机可读存储介质的实施例中,资源包括以下至少一项:经由网络可访问的电子邮件服务器;经由网络可访问的数据储存库;或者经由网络可访问的应用服务器。

[0102] 在该计算机可读存储介质的实施例中,该方法还包括:响应于确定计算设备不再合规,经由网络来将符合合规规则的新配置设置传输给计算设备。

[0103] 在该计算机可读存储介质的实施例中,触发事件包括以下至少一项:预定时间段的到期;从计算设备接收到的、计算设备的第二配置设置已经改变的指示;或者用户已经登录到计算设备的指示。

[0104] 在该计算机可读存储介质的实施例中,配置设置指定以下至少一项:待由计算设备实现的加密设置;待由计算设备实现的安全设置;或者需要被安装在计算设备上的应用或者操作系统中的至少一个的最低版本。

[0105] 在该计算机可读存储介质的实施例中,确定用于计算设备的配置设置包括:标识已经登录到计算设备的用户;以及确定与用户和计算设备相关联的配置设置。

[0106] V.结论

[0107] 虽然上面已经对各种实施例进行了描述,但是应该理解,它们仅通过示例的方式而非限制被呈现出来。对于相关领域的技术人员而言将明显的是:在不脱离实施例的精神和范围的情况下,可以在其中进行形式和细节上的各种改变。因此,实施例的广度和范围不应该受限于上述示例性实施例中的任何示例性实施例,而是应该仅根据以下权利要求书及其等效物被限定。

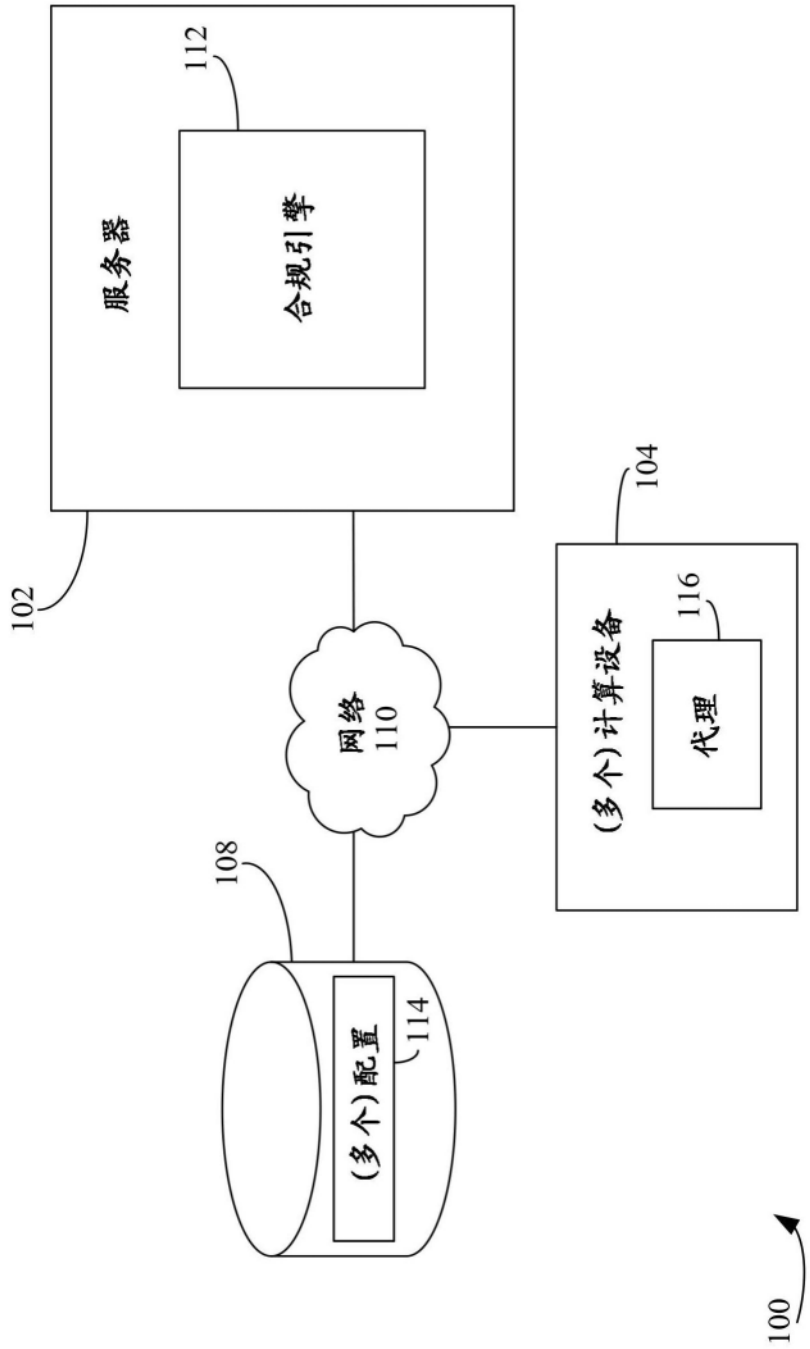


图1

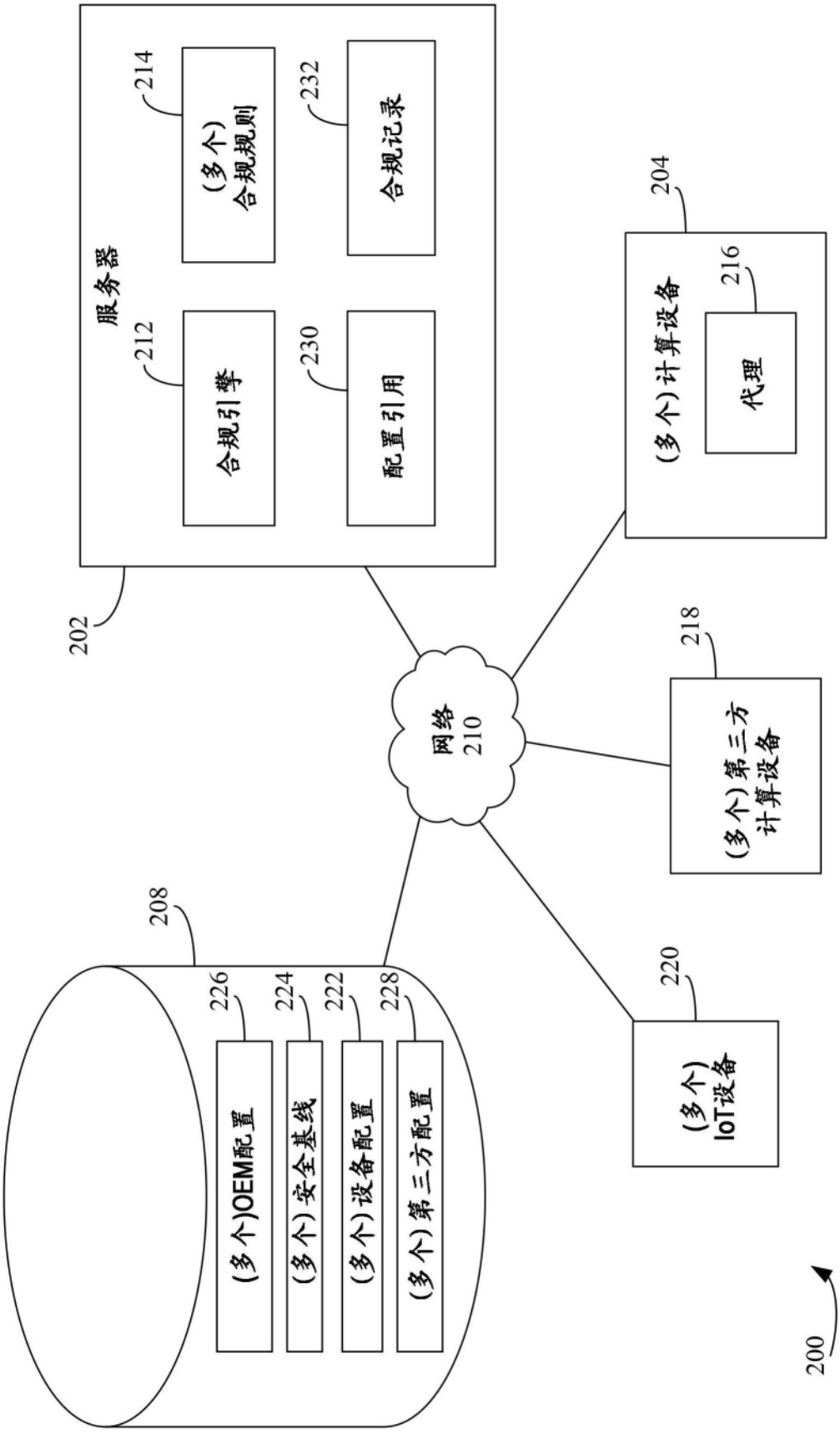

服务器
202
212
合规引擎
214
(多个)
合规规则
230
配置引用
232
合规记录
网络
210
204
(多个)计算设备
216
代理
218
(多个)第三方
计算设备
220
(多个)
IoT设备
208
226
(多个)OEM配置
224
(多个)安全基线
222
(多个)设备配置
228
(多个)第三方配置
200

图2

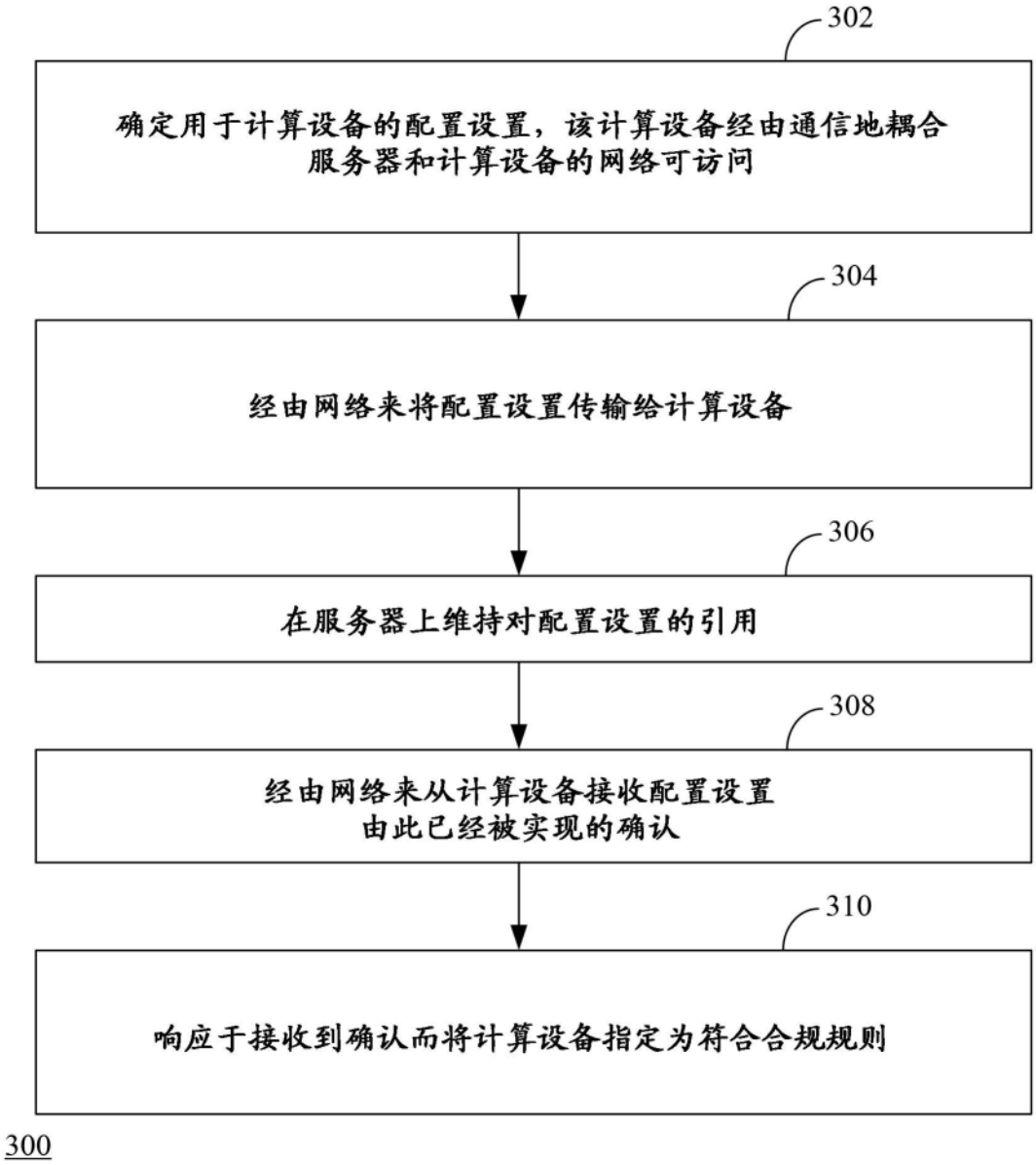

302
确定用于计算设备的配置设置，该计算设备经由通信地耦合服务器和计算设备的网络可访问
304
经由网络来将配置设置传输给计算设备
306
在服务器上维持对配置设置的引用
308
经由网络来从计算设备接收配置设置由此已经被实现的确认
310
响应于接收到确认而将计算设备指定为符合合规规则
300

图3

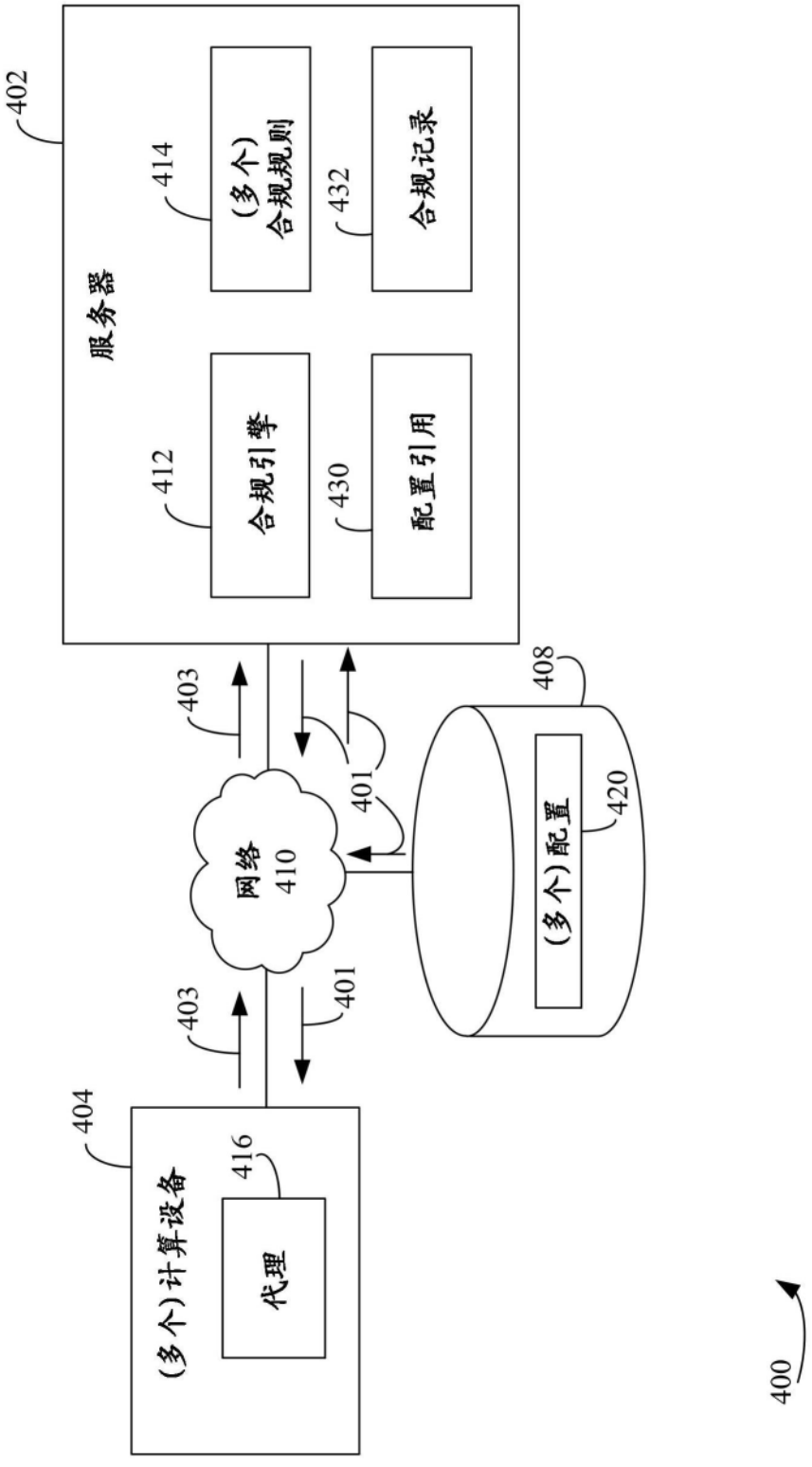

402
服务器
414
(多个)
合规规则
432
合规记录
412
合规引擎
430
配置引用
403
401
网络
410
408
(多个)配置
420
403
401
404
(多个)计算设备
416
代理
400

图4

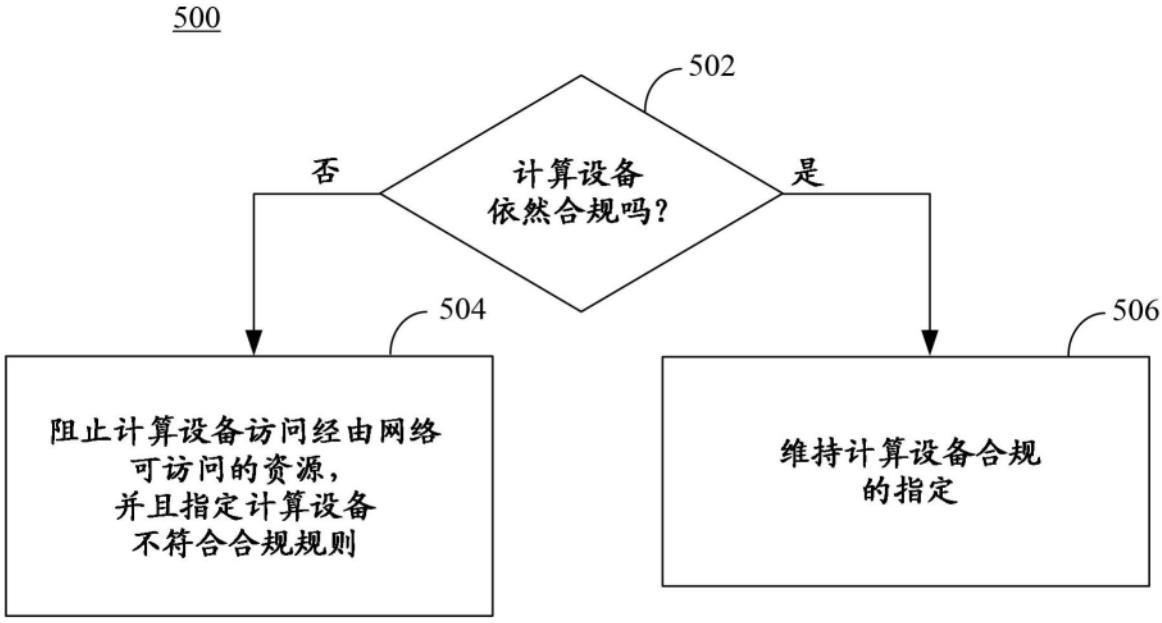

500
502
计算设备
依然合规吗?
否
是
504
506
阻止计算设备访问经由网络
可访问的资源,
并且指定计算设备
不符合合规规则
维持计算设备合规
的指定

图5

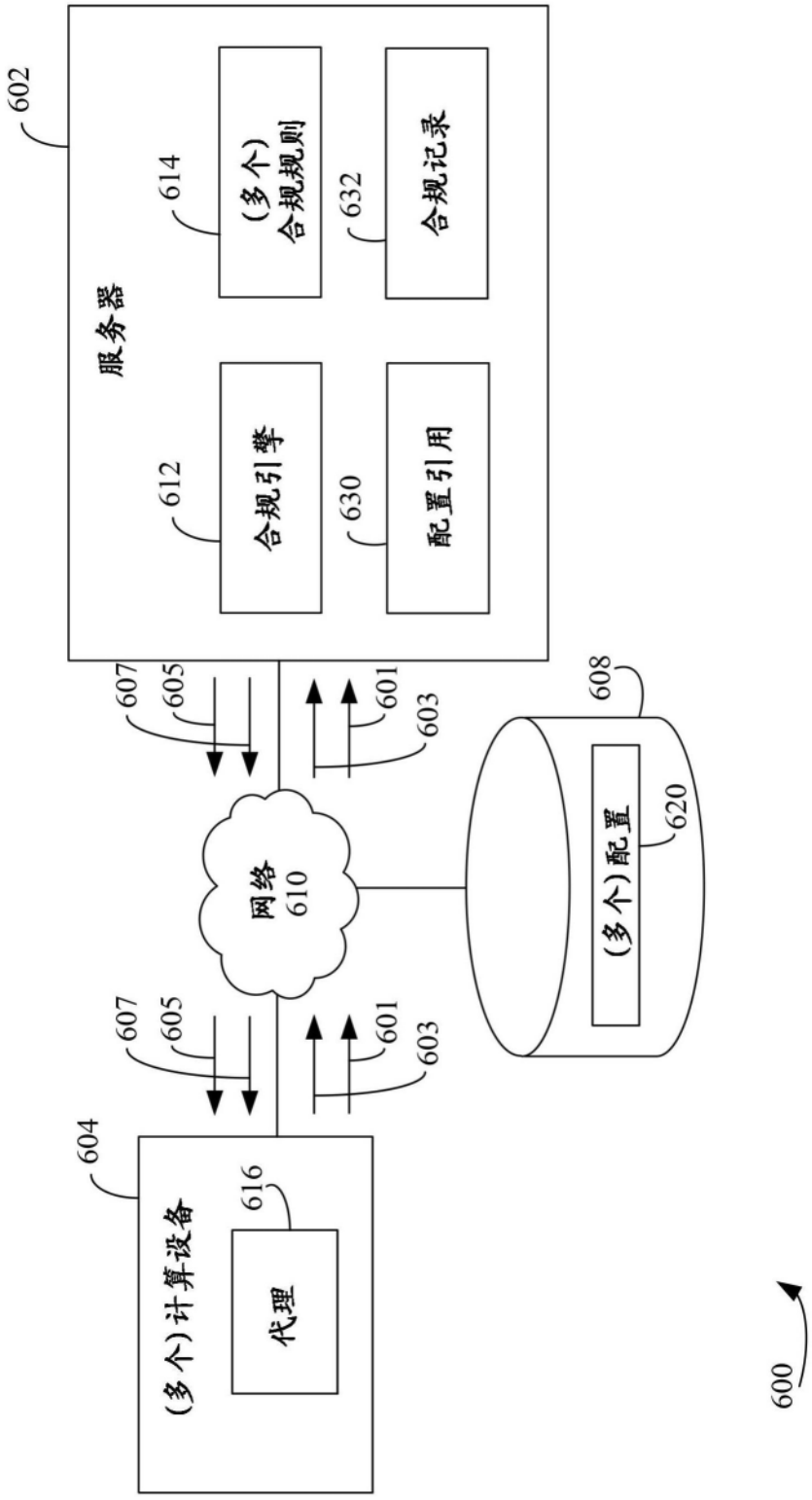

602
服务器
614
(多个)
合规规则
632
合规记录
612
合规引擎
630
配置引用
607
605
601
603
608
网络
610
(多个)配置
620
607
605
601
603
604
(多个)计算设备
616
代理
600

图6

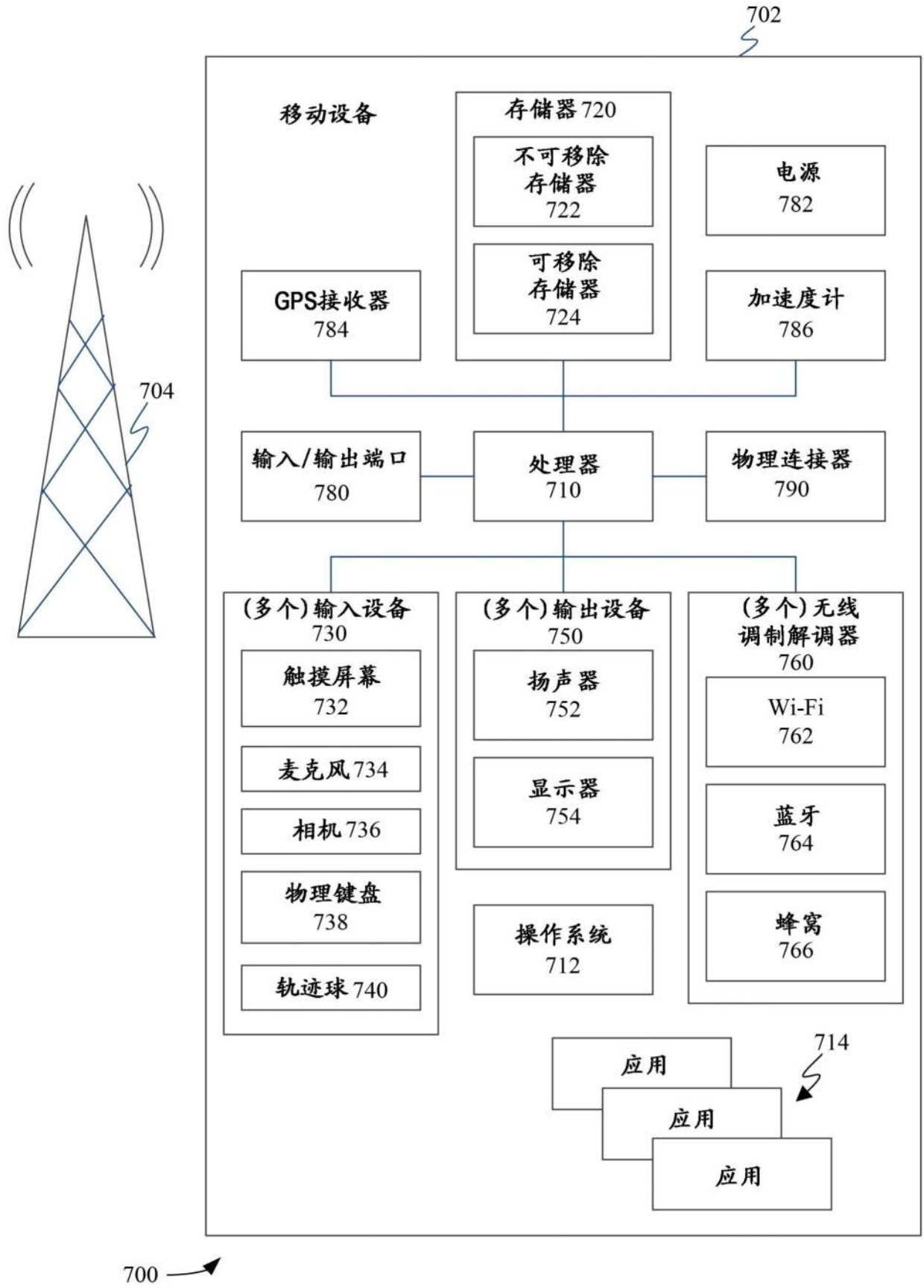

702
移动设备
存储器720
不可移除存储器722
可移除存储器724
电源782
GPS接收器784
加速度计786
704
输入/输出端口780
处理器710
物理连接器790
(多个)输入设备730
触摸屏幕732
麦克风734
相机736
物理键盘738
轨迹球740
(多个)输出设备750
扬声器752
显示器754
操作系统712
(多个)无线调制解调器760
Wi-Fi762
蓝牙764
蜂窝766
714
应用
应用
应用
700

图7

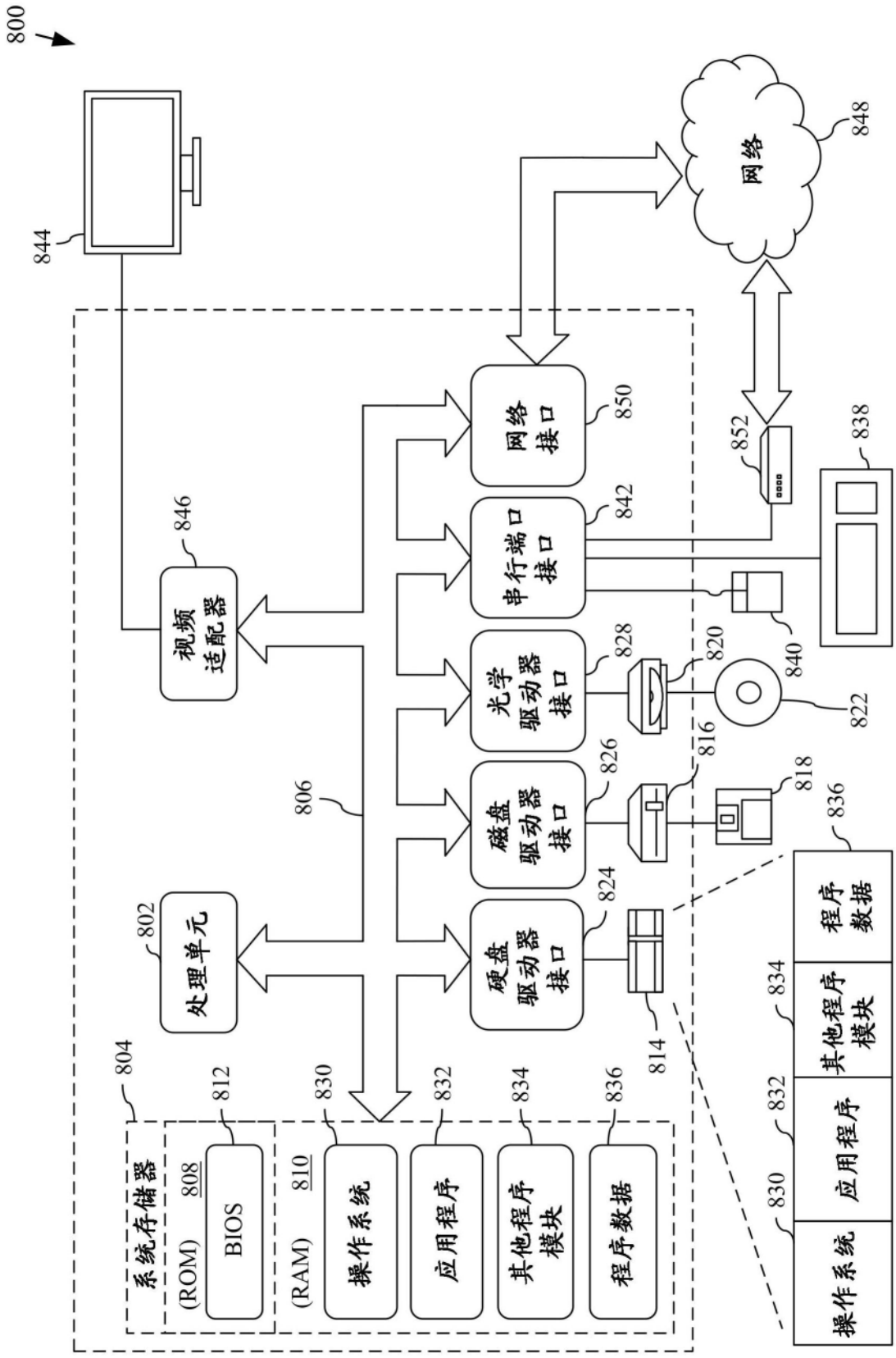

800
844
网络
848
处理单元
802
804
系统存储器
(ROM) 808
BIOS
812
(RAM) 810
操作系统
830
应用程序
832
其他程序模块
834
程序数据
836
806
视频适配器
846
网络接口
850
串行端口接口
842
852
838
光学驱动器接口
828
820
840
822
磁盘驱动器接口
826
816
818
硬盘驱动器接口
824
814
836
程序数据
834
其他程序模块
832
应用程序
830
操作系统

图8