(12) STANDARD PATENT (11) Application No. **AU 2013385810 B2**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
Time-based functionality restrictions

(51) International Patent Classification(s)
G06F 11/22 (2006.01) ***G06F 17/30*** (2006.01)
G06F 15/16 (2006.01)

(21) Application No: **2013385810** (22) Date of Filing: **2013.10.21**

(87) WIPO No: **WO14/168652**

(30) Priority Data

(31) Number	(32) Date	(33) Country
13/862,380	**2013.04.13**	**US**

(43) Publication Date: **2014.10.16**
(44) Accepted Journal Date: **2017.03.02**

(71) Applicant(s)
AirWatch LLC

(72) Inventor(s)
Marshall, John;Stuntebeck, Erich

(74) Agent / Attorney
FB Rice, L 14 90 Collins St, Melbourne, VIC, 3000, AU

(56) Related Art
US 2008/0228504
US 7107339

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 October 2014 (16.10.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/168652 A1

(51) International Patent Classification:
G06F 11/22 (2006.01) *G06F 17/30* (2006.01)
G06F 15/16 (2006.01)

(21) International Application Number:
PCT/US2013/065915

(22) International Filing Date:
21 October 2013 (21.10.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/862,380 13 April 2013 (13.04.2013) US

(71) Applicant: SKY SOCKET, LLC [US/US]; 1155 Perimeter Center West, Suite 100, Atlanta, GA 30338 (US).

(72) Inventors: MARSHALL, John; 943 Peachtree Street Northeast, Apartment #706, Atlanta, GA 30309 (US). STUNTEBECK, Erich; 3317 Chastain Ridge Drive, Marietta, GA 30066 (US).

(74) Agent: DIRICO, John; 1155 Perimeter Center West, Suite 100, Atlanta, GA 30338 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

[Continued on next page]

(54) Title: TIME-BASED FUNCTIONALITY RESTRICTIONS

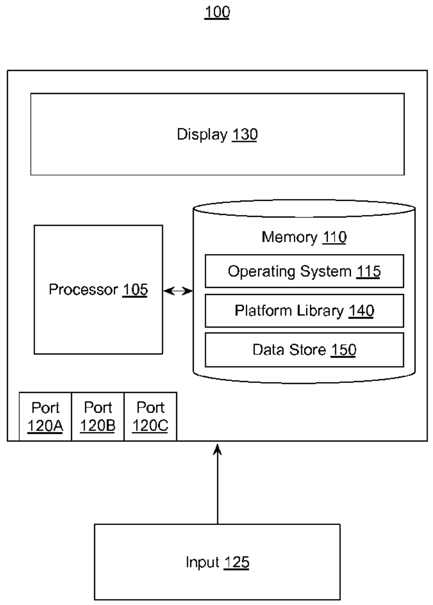

Figure 1

(57) Abstract: Time-based functionality restrictions may be provided. Periodic scans may be performed to identify requests to perform functions on user devices, to determine whether the functions are compliant with compliance rules associated with the user devices that specify time periods during which the user devices are authorized to perform the functions, and to perform remedial actions if the functions are not compliant with the compliance rules.

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

TITLE

TIME-BASED FUNCTIONALITY RESTRICTIONS

STATEMENT OF INCORPORATION BY REFERENCE

[0001] This application is a PCT Application claiming priority to US Application No. 13/862,380, filed on April 13, 2013. The patent application identified above is incorporated herein by reference in its entirety.

BACKGROUND

[0002] Today, many governments are implementing legislative penalties for businesses that provide their employees with access to business resources and/or device functionality outside of standard workday hours. Also, many businesses experience loss of revenue as a result of their employees' access to personal resources and/or device functionality during standard workday hours. Automated compliance rules may be provided for handling situations where certain functionality on a device is restricted during certain time periods, such as during and/or outside standard workday hours. Conventional solutions often restrict the use of a device entirely to prevent the device from performing such functionality that is restricted during such time periods.

[0002a] Any discussion of documents, acts, materials, devices, articles or the like which has been included in the present specification is not to be taken as an admission that any or all of these matters form part of the prior art base or were common general knowledge in the field relevant to the present disclosure as it existed before the priority date of each claim of this application.

[0002b] Throughout this specification the word "comprise", or variations such as "comprises" or "comprising", will be understood to imply the inclusion of a stated element, integer or step, or group of elements, integers or steps, but not the exclusion of any other element, integer or step, or group of elements, integers or steps.

SUMMARY

[0003] This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description.

[0003a] In a first aspect a method is provided, the method comprising for providing time-based functionality restrictions, the method being performed on a user device comprising at least one processor and at least one memory storage, the method comprising:

obtaining, from a compliance server, at least one compliance rule,

storing, on the user device, the at least one compliance rule,

identifying, using an agent application executing on the user device, at least one request to execute a particular application in the user device;

determining, using the agent application, whether the at least one request does not comply with the at least one compliance rule, wherein the at least one compliance rule comprises at least one time period when the user device is authorized to execute the application; and,

performing, using the agent application, at least one remedial action in response to at least one determination that the at least one request does not comply with the at least one compliance rule, wherein the remedial action comprises disabling access to the particular application by the user device and

in response to determining that the at least one request complies with the at least one compliance rule, initiating execution of the particular application.

[0003b] In another aspect, a user device is provided comprising:

at least one memory storage; and

at least one processor coupled to the at least one memory storage, wherein the at least one processor is configured to:

obtain, from a compliance server, at least one compliance rule;

store the at least one compliance rule on the user device;

identify, using an agent application executing on the user device, at least one request to execute a particular application by the user device;

determine, using the agent application, whether the at least one request does not comply with the least one compliance rule, wherein the at least one compliance rule comprises at least one time period when the user device is authorized to execute the particular application, wherein the remedial action comprises disabling access to the particular application by the user device,

perform, using the agent application, at least one remedial action in response to at least one determination that the at least one request does not comply with at least one of the at least one compliance rule , and

in response to determining that the at least one request complies with the at least one compliance rule, initiate execution of the particular application.

[0003c] In a further aspect, a non-transitory computer-readable medium is provided that stores a set of instructions that when executed by a user device comprising at least one processor and a memory storage performs a method according to the first aspect, or embodiments thereof.

[0004] Time-based functionality restrictions may be provided. Periodic scans may be performed to identify requested functionality and determine whether the functionality is restricted according to a time constraint. Upon identifying a request to perform functionality that is restricted according to a time constraint, the request to perform the functionality may be denied. The time constraints may be defined according to, amongst other possible time periods, standard workday hours.

[0005] It is to be understood that both the foregoing general description and the following Detailed Description are examples and explanatory only, and should not be considered to restrict the disclosure's scope, as described and claimed. Further, features and/or variations may be provided in addition to those set forth herein. For example, embodiments of the disclosure may be directed to various feature combinations and sub-combinations described in the Detailed Description.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] Many aspects of the present disclosure can be better understood with reference to the following diagrams. The drawings are not necessarily to scale. Instead, emphasis is placed upon clearly illustrating certain features of the disclosure. Moreover, in the drawings, like reference numerals designate corresponding parts throughout the several views. In the drawings:

[0007] Figure 1 is a block diagram of a user device;

[0008] Figure 2 is a block diagram of an operating environment; and

[0009] Figure 3 is a flow chart illustrating a method for providing time-based functionality restrictions.

DETAILED DESCRIPTION

[0010] The following Detailed Description refers to the accompanying Figures. Wherever possible, the same reference numbers are used in the Figures and the following description to refer to the same or similar elements. While embodiments of the disclosure may be described, modifications, adaptations, and other implementations are possible. For example, substitutions, additions, or modifications may be made to the elements illustrated in the Figures, and the methods described herein may be modified by substituting, reordering, or adding stages to the disclosed methods. Accordingly, the following Detailed Description does not limit the disclosure. Instead, the proper scope of the disclosure is defined by the appended claims.

[0011] Time-based functionality restrictions may be provided by certain methods, apparatuses, and non-transitory computer readable medium as described herein. Methods for providing time-based functionality restrictions may include methods performed by software applications. Examples of such methods may include those performed by device management server applications executed on servers and device management agent applications executed on user devices. User devices may include smartphones, tablets, laptops, desktops and other computing devices. Moreover, apparatuses for providing time-based functionality restrictions may include devices executing software applications that perform methods for providing time-based functionality restrictions. Examples of such apparatuses may include servers executing device management server applications and user devices executing device management agent applications. Additionally, non-transitory computer readable mediums for providing time-based functionality restrictions may include software applications that when executed cause a computing device to perform the steps of the methods for providing time-based functionality restrictions. Examples of such non-transitory computer readable mediums may include device management server applications executable by servers and device management agent applications executable by user devices.

[0012] Providing time-based functionality restrictions may begin by identifying requests to perform functions on user devices and/or identifying functions being performed on user devices. Compliance rules associated with the user devices may be identified and, based on such compliance rules, a determination may be made as to whether the functions requests and/or being performed are authorized to be performed by the user devices at the current time. If it is determined that the user devices are not authorized to perform the functions at the current time, a remedial action may be performed such as blocking the function being requested and/or being performed. If it is determined a second time that the users are not authorized to perform the functions at the current time, an escalated remedial action may be taken such as erasing business and/or personal data from the user device. Furthermore, if it is determined that the user devices are authorized to perform the functions at the current time, the user devices may be permitted to proceed with the request to perform functions and/or the functions being performed without interruption.

[0013] Time-based functionality restrictions may be implemented to enable and/or disable certain functionality on a user device during and/or outside of standard workday hours. For example, time-based functionality restrictions may ensure that employees only receive their business email on their smartphone during workdays and only receive their personal email on their smartphone outside workdays.

[0014] Figure 1 is a block diagram of a User Device 100 comprising a Processor 105 and a Memory 110. Depending on the configuration and type of User Device, Memory 110 may comprise, but is not limited to, volatile (e.g. random access memory (RAM)), non-volatile (e.g. read-only memory (ROM)), flash memory, or any combination thereof. Memory 110 may store executable programs and related data components of various applications and modules for execution by User Device 100. Memory 110 may be coupled to Processor 105 for storing configuration data and operational parameters, such as commands that are recognized by Processor 105. User Device 100 may comprise, for example, a desktop computer, a laptop computer, a personal digital assistant, a cellular telephone, a set-top box, a music player, a web pad, a tablet computer system, a game console, and/or another device with like capability.

[0015] Basic functionality of User Device 100 may be provided by an Operating System 115 contained in Memory 100. Various programmed software applications may be executed by utilizing the computing resources in User Device 100. Applications stored in Memory 110 may be executed by Processor 105 (e.g., a central processing unit or digital signal processor) under the auspices of Operating System 115. For example, Processor 105 may be configured to execute applications such as web browsing applications, email applications, instant messaging applications, and/or other applications capable of receiving and/or providing data.

[0016] Data provided as input to and generated as output from the application(s) may be stored in Memory 110 and read by Processor 105 from Memory 110 as needed during the course of application program execution. Input data may be data stored in Memory 110 by a secondary application or other source, either internal or external to User Device 100, or possibly anticipated by the application and thus created with the application program at the time it was generated as a software application program. Data may be received via any of a plurality of (Communication) Ports 120A, 120B, and/or 120C of User Device 100. Communication Ports 120A, 120B, and/or 120C may allow User Device 100 to communicate with other devices, and may comprise components such as an Ethernet network adapter, a modem, and/or a wireless network connectivity interface. For example, the wireless network connectivity interface may comprise one and/or more of a PCI (Peripheral Component Interconnect) card, USB (Universal Serial Bus) interface, PCMCIA (Personal Computer Memory Card International Association) card, SDIO (Secure Digital Input-Output) card, NewCard, Cardbus, a modem, a wireless radio transceiver, and/or the like.

[0017] User Device 100 may also receive data as user input via an Input (Component) 125, such as a keyboard, a mouse, a pen, a stylus, a sound input device, a touch input device, a capture device, etc. A capture device may be operative to record user(s) and capture spoken words, motions and/or gestures, such as with a camera, microphone, and/or accelerometer. The capture device may comprise any speech and/or motion detection device capable of detecting the speech and/or actions of the user(s).

[0018] Data generated by applications may be stored in Memory 110 by the Processor 105 during the course of application program execution. Data may be provided to the user of User Device 100 during application program execution by means of a Display 130. Consistent with embodiments of this disclosure, Display 130 may comprise an integrated display screen and/or an output port coupled to an external display screen.

[0019] Memory 110 may also comprise a Platform Library 140. Platform Library 140 may comprise a collection of functionality useful to multiple applications, such as may be provided by an application programming interface (API) to a software development kit (SDK). These utilities may be accessed by applications as necessary so that each application does not have to contain these utilities thus allowing for memory consumption savings and a consistent user interface.

[0020] Furthermore, embodiments of this disclosure may be practiced in conjunction with a graphics library, other operating systems, or any other application program and is not limited to any particular application or system. The devices described with respect to the Figures may have additional features or functionality. For example, User Device 100 may also include additional data storage devices (removable and/or non-removable) such as, for example, magnetic disks, optical disks, or tape (not shown).

[0021] User Device 100 may store device and/or user-specific information in a Data Store 150, such as a device profile, a plurality of credentials and/or a plurality of user preferences. A device profile may comprise an indication of the current position of User Device 100 and/or indications of the hardware, software, and security attributes that describe User Device 100. For instance, the device profile may represent hardware specifications of User Device 100, version and configuration information of various software program and hardware components installed on User Device 100, data transmission protocols enabled on User Device 100, version and usage information of various resources stored on User Device 100, and/or any other attributes associated with the state of User Device 100. The device profile may further comprise data indicating a date of last virus scan of User Device 100, a date of last access by an IT representative, a date of last service by the IT representative, and/or any other data indicating maintenance and usage of User Device 100. Furthermore, the device profile may comprise indications of the past behavior of associated users, such as resources accessed, charges for resources accessed, and the inventory accessed from such resources.

[0022] The credentials may comprise a plurality of user credentials and/or a plurality of device credentials. The user credentials may comprise a plurality of PIN numbers, simple passwords, complex passwords, usernames, account identifiers, biometric indicators, and/or other data capable of authenticating the user of the User Device 100. The device credentials may comprise a plurality of hardware identifiers, serial numbers, IMEI numbers, phone numbers, and/or other data capable of authenticating the User Device 100. The user preferences may comprise a listing of factors that may affect the experience of the user of User Device 100. In particular, the user preferences may include indications of the user's age, gender, bodily traits, preferred resource types, preferred venue resources, and combinations thereof.

[0023] Figure 2 is a block diagram view of an operating environment 200 comprising User Device 100 in communication with a Compliance Server 220 via a Network 240. The Compliance Server 220 may comprise, for example, cloud-based solutions, server computers and/or any other system providing device management capability. For purposes of convenience, the Compliance Server 220 is referred to herein in the singular, although it is understood that a plurality of servers may be employed in the arrangements as descried herein. Furthermore, in some embodiments, multiple Compliance Servers 220 may operate on the same server computer. The components executed on the Compliance Server 220, for example, may comprise various applications, services, processes, systems, engines, or functionality not disclosed in detail herein.

[0024] The Compliance Server 220 may comprise a Rules Store 230 comprising a plurality of compliance rules that may be applicable to User Device 100. While the Rules Store 230 is shown as within the Compliance Server 220, the Rules Store 230 may alternately be within the User Device 100 and may be remotely updated periodically by Compliance Server 220 according to common over-the-air (OTA) updating methods. Attempts by User Device 100 to perform certain functionality on User Device 100 may require User Device 100 to be in compliance with one and/or more of the compliance rules. Depending on the sensitivity of a given functionality, different compliance rules may be necessary to ensure that the functionality is adequately restricted. Some functionality may only require ensuring that the proper user is requesting the functionality. Other resources may require compliance with more stringent authorization rules, such as determining whether the functionality is restricted during certain time windows. Accordingly, User Device 100 and/or Compliance Server 220 may be operative to determine whether the user of User Device 100 is authorized to perform requested functionality at the time the user requests to perform such functionality.

[0025] In some embodiments, an agent application executed on User Device 100 may make the compliance determination based on the device profile, credentials, and/or user preferences. For instance, an agent application may monitor the calls by applications on User Device 110 to the Operating System 115 of User Device 100 to determine whether User Device 110 seeks to perform functionality that may violate a given compliance rule. Additionally, an agent application on User Device 100 may approve and/or deny the associated functionality requests. For instance, the agent application may instruct Operating System 115 on User Device 100 to disable the camera of User Device 120 in response to a determination that a compliance rule specifies that the camera cannot be used at the time of the request by the User Device 100 to operate the camera.

[0026] In some embodiments, an agent application executed on User Device 100 may rely on Compliance Server 220 to determine whether a given functionality request on User Device 100 is permitted according to the compliance rules. For instance, the agent application may transmit a functionality request, a device profile, credentials, and/or user preferences to Compliance Server 220 so that Compliance Server 220 may determine whether User Device 110 seeks to perform functionality that may violate a given compliance rule. Additionally, Compliance Server 220 may approve and/or deny the associated functionality requests. For instance, Compliance Server 220 may instruct an agent application on User Device 100 to instruct Operating System 115 on User Device 100 to disable the email transmission port of User Device 120 in response to a determination that a compliance rule specifies that email cannot be received at the time of the request by the User Device 100 to receive email. Compliance Server 220 may, for instance, instruct an agent application and/or Operating System 115 of User Device 100 via application programming interface (API) calls and/or other programming that allows control and/or instruction of User Device 100 by applications and/or services communicatively coupled to User Device 100.

[0027] In some embodiments, the compliance rules may comprise device settings and/or executable instructions that define which functionality the Operating System 115 of User Device 100 is authorized to perform at a given time. In certain embodiments, the compliance rules may specify that functionality related to personal use of User Device 100 may not be performed during standard workday hours, and/or that functionality related to business use of User Device 100 may not be performed outside standard workday hours. For example, the compliance rules may specify that business applications may only be executed on User Device 100 between 9AM and 5PM on weekdays, and may specify that personal applications may only be executed on User Device 100 between 5PM and 9AM on weekdays and/or anytime on weekends. Furthermore, the compliance rules may comprise a list of functions, such as those provided by APIs associated with Operating System 115 and/or Platform Library 140, that may be treated as protected functions. Calls to these functions, such as calls to retrieve login credentials, may result in checks by User Device 100 and/or Compliance Server 220 for compliance with the compliance rules.

[0028] The Network 240 may comprise, for example, any type of wired and/or wireless network such as a wireless local area network (WLAN), a wireless wide area network (WWAN), Ethernet, fiber-optic network, and/or any other type of wired and/or wireless network now known or later developed. Additionally, the Network 240 may be or include the Internet, intranets, extranets, microwave networks, satellite communications, cellular systems, PCS, infrared communications, global area networks, or other suitable networks, etc., or any combination of such networks.

[0029] Figure 3 is a flow chart setting forth the general stages involved in a method 300 consistent with embodiments of this disclosure for providing time-based functionality restrictions. Ways to implement the stages of method 300 will be described in greater detail below. For purposes of illustration, not limitation, method 300 is described with respect to User Device 100 in communication with Compliance Server 220. Method 300 may begin at starting block 305 and proceed to stage 310 and identify requests to perform functions on a User Device 100 and/or functions being performed on a User Device 100. For example, a request to access business email on a User Device 100 may be identified in stage 310.

[0030] From stage 310, method 300 may advance to stage 315 where method 300 identifies a plurality of compliance rules associated with the User Device 100. In some embodiments, the compliance rules may specify at least one time period when the User Device 100 is authorized to perform a given function. Examples of compliance rules include compliance rules that specify that business functions may only be accessed during business hours and compliance rules that specify that personal functions may only be accessed during personal hours. From stage 315, method 300 may advance to stage 320 where method 300 determines whether the functions associated with the User Device 100 comply with the compliance rule associated with the User Device 100. For instance, a request to access a business email account on User Device 100 outside of workday hours would not comply with a compliance rule specifying that User Device 100 is only authorized to access business email accounts during workday hours.

[0031] If it is determined that the functions do not comply with the compliance rules, method 300 may advance to stage 330 and perform a remedial action. Remedial actions may be taken on a User Device 100 and/or remote services communicatively coupled to a User Device 100. Remedial actions may include disabling hardware features of a User Device 100, disabling software features of a User Device 100, disabling applications of a User Device 100, erasing the contents of memory locations of a User Device 100, restoring a User Device 100 to its factory state, and queuing a function until a User Device 100 is authorized to perform the function. Disabling hardware features of a User Device 100 may include disabling the Camera, Microphone and/or other features of a User Device 100 that are available on User Device 100. Disabling software features of a User Device 100 may include disabling Siri and/or other software features provided by Operating System 115 and/or other factory-installed software of User Device 100. Disabling applications of a User Device 100 may include uninstalling and/or blocking execution of applications of a User Device 100, such as email applications, browser applications, content management applications, application stores and/or the like.

[0032] Erasing the contents of memory locations may include content associated with business data, where business data may include electronic files, applications and/or other data associated with an enterprise, business, and/or other organization. Erasing the contents of memory locations may also include content associated with personal data, where personal data may include electronic files, applications and/or other data that is not owned by and/or otherwise exclusively claimed and/or controlled by an enterprise, business and/or other organization. Restoring a User Device 100 to its factory state may include erasing the contents of all memory locations associated with data that was not present when the User Device 100 left the manufacturer and/or factory. Furthermore, remedial actions may be taken with respect to remote services communicatively coupled to a User Device 100, such as by blocking data transmissions from a User Device 100 to a remote service, blocking data transmissions from a remote service to a User Device 100, and erasing the contents of memory locations of a remote service. Once a remedial action is performed, method 300 may end at stage 335.

[0033] In some instances, the method 300 may repeat stage 330 to determine whether the functions that previously did not comply with the compliance rules now comply with the compliance rules. If it is determined that the functions, once again, do not comply with the compliance rules, the method 300 may perform at least one escalated remedial action. Certain remedial actions, such as erasing the contents of memory locations of a User Device 100 and restoring a User Device 100 to its factory state, may be more drastic than the other remedial actions disclosed and thereby classified as escalated remedial actions in such embodiment. Accordingly, if a function does not comply with the compliance rules for a second or subsequent time, an escalated remedial action may be performed. Once an escalated remedial action is performed, method 300 may end at stage 335.

[0034] If the function complies with the compliance rules at stage 320, method 300 may advance to stage 330 and approve the requests to perform functions on a User Device 100 and/or the functions being performed on a User Device 100. For instance, the requests to perform functions and/or the functions being performed may be approved by no action being taken by the method 300. Upon completion of stage 330, method 300 may end at stage 335.

[0035] The embodiments and functionalities described herein may operate via a multitude of computing systems, including wired and wireless computing systems, mobile computing systems (e.g., mobile telephones, tablet or slate type computers, laptop computers, etc.). In addition, the embodiments and functionalities described herein may operate over distributed systems, where application functionality, memory, data storage and retrieval and various processing functions may be operated remotely from each other over a distributed computing network, such as the Internet or an intranet. User interfaces and information of various types may be displayed via on-board computing device displays or via remote display units associated with one or more computing devices. For example, user interfaces and information of various types may be displayed and interacted with on a wall surface onto which user interfaces and information of various types are projected.

Interaction with the multitude of computing systems with which embodiments of this disclosure may be practiced include, keystroke entry, touch screen entry, voice or other audio entry, gesture entry where an associated computing device is equipped with detection (e.g., camera) functionality for capturing and interpreting user gestures for controlling the functionality of the computing device, and the like. The Figures above and their associated descriptions provide a discussion of a variety of operating environments in which embodiments of this disclosure may be practiced. However, the devices and systems illustrated and discussed with respect to the Figures are for purposes of example and illustration and are not limiting of a vast number of computing device configurations that may be utilized for practicing embodiments of this disclosure as described herein.

[0036] The term computer readable media as used herein may include computer storage media. Computer storage media may include volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information, such as computer readable instructions, data structures, program modules, or other data. System memory, removable storage, and non-removable storage are all computer storage media examples (i.e., memory storage.) Computer storage media may include, but is not limited to, RAM, ROM, electrically erasable read-only memory (EEPROM), flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store.

[0037] The term computer readable media as used herein may also include communication media. Communication media may be embodied by computer readable instructions, data structures, program modules, or other data in a modulated data signal, such as a carrier wave or other transport mechanism, and includes any information delivery media. The term “modulated data signal” may describe a signal that has one or more characteristics set or changed in such a manner as to encode information in the signal. By way of example, and not limitation, communication media may include wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, radio frequency (RF), infrared, and other wireless media.

[0038] A number of applications and data files may be used to perform processes and/or methods as described above. The aforementioned processes are examples, and a processing unit may perform other processes. Other programming modules that may be used in accordance with embodiments of this disclosure may include electronic mail, calendar, and contacts applications, data processing applications, word processing applications, spreadsheet applications, database applications, slide presentation applications, drawing or computer-aided application programs, etc.

[0039] Generally, consistent with embodiments of this disclosure, program modules may include routines, programs, components, data structures, and other types of structures that may perform particular tasks or that may implement particular abstract data types. Moreover, embodiments of the disclosure may be practiced with other computer system configurations, including hand-held devices, multiprocessor systems, microprocessor-based or programmable consumer electronics, minicomputers, mainframe computers, and the like. Embodiments of this disclosure may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

[0040] Furthermore, embodiments of this disclosure may be practiced in an electrical circuit comprising discrete electronic elements, packaged or integrated electronic chips containing logic gates, a circuit utilizing a microprocessor, or on a single chip containing electronic elements or microprocessors. Embodiments of this disclosure may also be practiced using other technologies capable of performing logical operations such as, for example, AND, OR, and NOT, including but not limited to mechanical, optical, fluidic, and quantum technologies. In addition, embodiments of the disclosure may be practiced within a general-purpose computer or in any other circuits or systems.

[0041] Embodiments of this disclosure may, for example, be implemented as a computer process and/or method, a computing system, an apparatus, device, or appliance, and/or as an article of manufacture, such as a computer program product or computer readable media. The computer program product may be a computer storage media readable by a computer system and encoding a computer program of instructions for executing a computer process. The computer program product may also be a propagated signal on a carrier readable by a computing system and encoding a computer program of instructions for executing a computer process. Accordingly, the present disclosure may be embodied in hardware and/or in software (including firmware, resident software, micro-code, etc.). In other words, embodiments of the present disclosure may take the form of a computer program product on a computer-usable or computer-readable storage medium having computer-usable or computer-readable program code embodied in the medium for use by or in connection with an instruction execution system. A computer-usable or computer-readable medium may be any medium that can contain, store, communicate, propagate, or transport the program for use by or in connection with the instruction execution system, apparatus, or device.

[0042] The computer-usable or computer-readable medium may be, for example but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, device, or propagation medium. More specific computer-readable medium examples (a non-exhaustive list), the computer-readable medium may include the following: an electrical connection having one or more wires, a portable computer diskette, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), an optical fiber, and a portable compact disc read-only memory (CD-ROM). Note that the computer-usable or computer-readable medium could even be paper or another suitable medium upon which the program is printed, as the program can be electronically captured, via, for instance, optical scanning of the paper or other medium, then compiled, interpreted, or otherwise processed in a suitable manner, if necessary, and then stored in a computer memory.

[0043] Embodiments of this disclosure may be practiced via a system-on-a-chip (SOC) where each and/or many of the elements described above may be integrated onto a single integrated circuit. Such an SOC device may include one or more processing units, graphics units, communications units, system virtualization units and various application functionalities, all of which may be integrated (or "burned") onto the chip substrate as a single integrated circuit. When operating via an SOC, the functionality, described herein, with respect to training and/or interacting with any element may operate via application-specific logic integrated with other components of the computing device/system on the single integrated circuit (chip).

[0044] Embodiments of this disclosure are described above with reference to block diagrams and/or operational illustrations of methods, systems, and computer program products according to embodiments of the disclosure. The functions/acts noted in the blocks may occur out of the order as shown in any flowchart. For example, two blocks shown in succession may in fact be executed substantially concurrently or the blocks may sometimes be executed in the reverse order, depending upon the functionality/acts involved.

[0045] While certain embodiments have been described, other embodiments may exist. Furthermore, although embodiments of the present disclosure have been described as being associated with data stored in memory and other storage mediums, data can also be stored on or read from other types of computer-readable media, such as secondary storage devices, like hard disks, floppy disks, or a CD-ROM, a carrier wave from the Internet, or other forms of RAM or ROM. Further, the disclosed methods' stages may be modified in any manner, including by reordering stages and/or inserting or deleting stages, without departing from the disclosure.

[0046] Embodiments of the present disclosure, for example, are described above with reference to block diagrams and/or operational illustrations of methods, systems, and computer program products according to embodiments of the disclosure. The functions/acts noted in the blocks may occur out of the order as shown in any flowchart. For example, two blocks shown in succession may in fact be executed substantially concurrently or the blocks may sometimes be executed in the reverse order, depending upon the functionality/acts involved.

[0047] While certain embodiments of the disclosure have been described, other embodiments may exist. Furthermore, although embodiments of the present disclosure have been described as being associated with data stored in memory and other storage mediums, data can also be stored on or read from other types of computer-readable media, such as secondary storage devices, like hard disks, floppy disks, or a CD-ROM, a carrier wave from the Internet, or other forms of RAM or ROM. Further, the disclosed methods' stages may be modified in any manner, including by reordering stages and/or inserting or deleting stages, without departing from the disclosure.

[0048] All rights including copyrights in the code included herein are vested in and the property of the Assignee. The Assignee retains and reserves all rights in the code included herein, and grants permission to reproduce the material only in connection with reproduction of the granted patent and for no other purpose.

[0049] While the specification includes examples, the disclosure's scope is indicated by the following claims. Furthermore, while the specification has been described in language specific to structural features and/or methodological acts, the claims are not limited to the features or acts described above. Rather, the specific features and acts described above are disclosed as example for embodiments of the disclosure.

[0050] Technical effects of the present disclosure may include leveraging client devices to aide in legal compliance, as certain legal compliance requirements may prohibit employees from performing employment-related tasks when the current time is outside of certain authorized employment time windows. Technical effects of the present disclosure may further include benefits to the performance of client devices for personal tasks when the current time is outside of certain authorized employment time windows, as removing access to functionality and/or resources associated with employment may permit an increase in the allocation of memory and/or processor power allotted to such personal tasks.

2013385810 24 Jan 2017

CLAIMS:

1. A method comprising for providing time-based functionality restrictions, the method being performed on a user device comprising at least one processor and at least one memory storage, the method comprising:

obtaining, from a compliance server, at least one compliance rule,

storing, on the user device, the at least one compliance rule,

identifying, using an agent application executing on the user device, at least one request to execute a particular application in the user device;

determining, using the agent application, whether the at least one request does not comply with the at least one compliance rule, wherein the at least one compliance rule comprises at least one time period when the user device is authorized to execute the application; and,

performing, using the agent application, at least one remedial action in response to at least one determination that the at least one request does not comply with the at least one compliance rule, wherein the remedial action comprises disabling access to the particular application by the user device and

in response to determining that the at least one request complies with the at least one compliance rule, initiating execution of the particular application.

2. The method of claim 1, wherein the at least one request does not comply with the at least one compliance rule if the at least one request does not comply with the at least one compliance rule at the time that the at least one request was initiated.

3. The method of any of claims 1 or 2, wherein the at least one compliance rule comprises a plurality of compliance rules and the determination that the at least one request does not comply with at least one of the at least one compliance rule comprises:

a determination that the at least one request does not comply with a threshold number of the plurality of compliance rules or a determination that the at least one request does not comply with each of the plurality of compliance rules.

4. The method of any of claims 1 to 3, wherein the at least one remedial action further comprises at least one of:

disabling at least one hardware feature of the user device;

disabling at least one software feature of the user device; queuing the at least one request to execute the particular application on the user device until the at least one request complies with the at least one compliance rule; or

restoring the user device to its factory state.

5. The method of any of claims 1 to 4, wherein the at least one remedial action further comprises erasing at least one location of at least one memory of the user device.

6. The method of claim 5, wherein the at least one location of the at least one memory of the user device comprises:

data associated with the at least one request;

data associated with the particular application;

business data; or personal data.

7. The method of any of claims 1 to 6, wherein the at least one remedial action further comprises at least one remedial action taken with respect to at least one remote service communicatively coupled to the user device.

8. The method of any of claims 1 to 7, wherein the at least one remedial action further comprises blocking at least one data transmission from the user device to at least one remote service communicatively coupled to the user device.

9. The method of any of claims 1 to 8, wherein the at least one remedial action further comprises blocking at least one data transmission from at least one remote service communicatively coupled to the user device to the user device.

10. The method of any of claims 1 to 9, wherein the at least one remedial action further comprises erasing at least one location of at least one memory of at least one remote service communicatively coupled to the user device.

11. The method of any of claims 1 to 10, further comprising

determining whether the requests that previously did not comply with the at least one compliance rule now comply with the at least one compliance rule and

performing an escalated remedial action in response to a determination that the request once again does not comply with the at least one compliance rule.

12. A user device comprising:

at least one memory storage; and

at least one processor coupled to the at least one memory storage, wherein the at least one processor is configured to:

obtain, from a compliance server, at least one compliance rule;

store the at least one compliance rule on the user device;

identify, using an agent application executing on the user device, at least one request to execute a particular application by the user device;

determine, using the agent application, whether the at least one request does not comply with the least one compliance rule, wherein the at least one compliance rule comprises at least one time period when the user device is authorized to execute the particular application, wherein the remedial action comprises disabling access to the particular application by the user device

perform, using the agent application, at least one remedial action in response to at least one determination that the at least one request does not comply with at least one of the at least one compliance rule , and

in response to determining that the at least one request complies with the at least one compliance rule, initiate execution of the particular application.

13. The user device of claim 12, wherein the at least one processor is configured to identify the at least one request by the user device on a periodic basis which comprises a configurable setting defined by at least one administrator of the apparatus.

14. The user device of any of claims 12 or 13, wherein the at least one processor is configured to identify the at least one request by the user device at the request of at least one administrator of the apparatus.

15. The user device of any of claims 12 to 14, wherein the at least one compliance rule comprises a plurality of compliance rules and the determination that the at least one request does not comply with at least one of the at least one compliance rule comprises:

a determination that the at least one request does not comply with a threshold number of the at least one compliance rule or a determination that the at least one request does not comply with each of the plurality of compliance rules.

16. The user device of any of claims 12 to 15, wherein the at least one remedial action further comprises:

disabling at least one hardware feature of the at least one user device;

disabling at least one software feature of the at least one user device; or

disabling at least one application of the user device.

17. The user device of any of claims 12 to 16, wherein the at least one remedial action further comprises erasing at least one location of at least one memory of the user device, wherein the location comprises business data or personal data.

18. The user device of any of claims 12 to 17, wherein the at least one remedial action further comprises:

restoring the user device to its factory state; or queuing the at least one request until the at least one request complies with the at least one compliance rule.

19. The user device of any of claims 12 to 18, wherein the at least one remedial action further comprises:

blocking at least one data transmission from the user device to at least one remote service communicatively coupled to the user device; blocking at least one data transmission from at least one remote service communicatively coupled to the user device to the user device or erasing at least one location of at least one memory of at least one remote service communicatively coupled to the user device .

20. A non-transitory computer-readable medium that stores a set of instructions that when executed by a user device comprising at least one processor and a memory storage performs the method of any one of claims 1 to 11

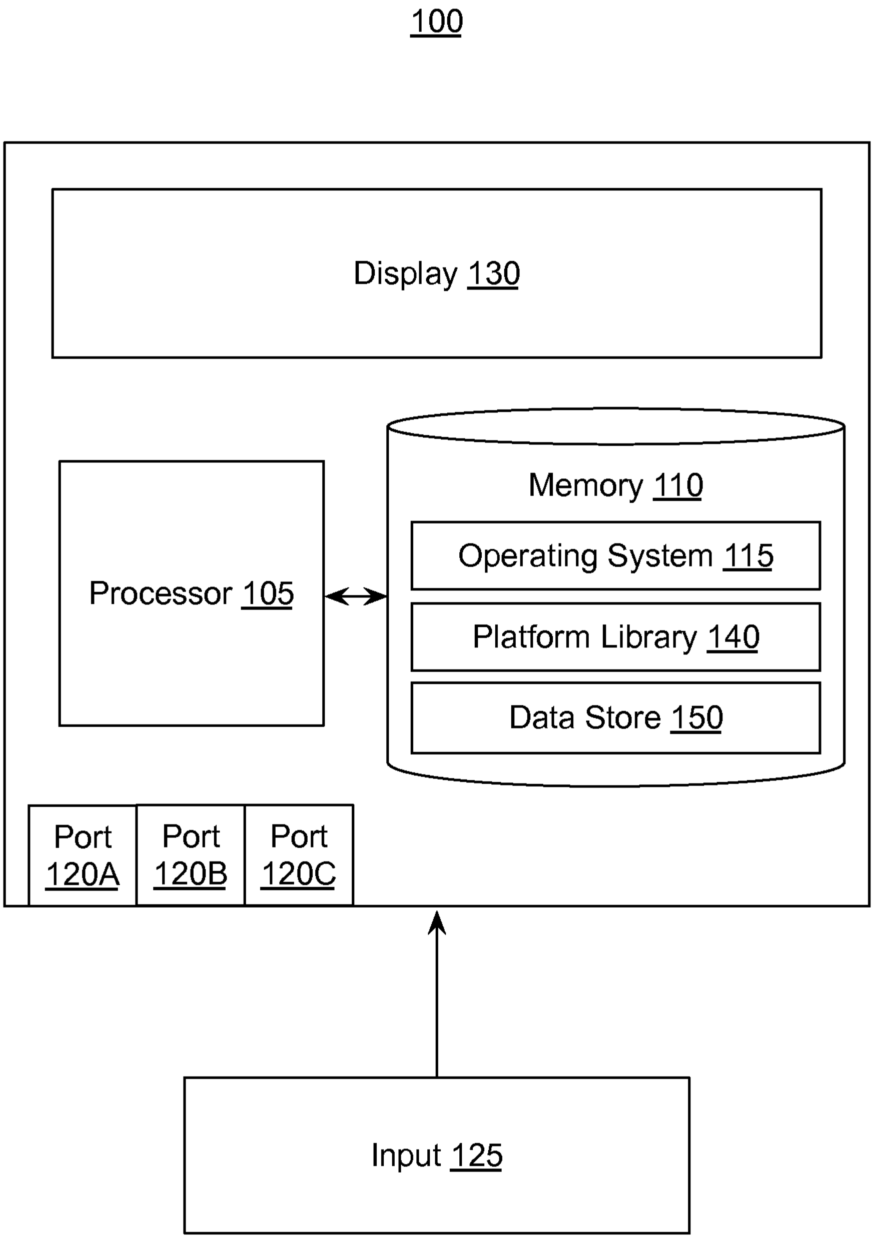
100
Display 130
Memory 110
Operating System 115
Platform Library 140
Data Store 150
Processor 105
Port 120A
Port 120B
Port 120C
Input 125

Figure 1

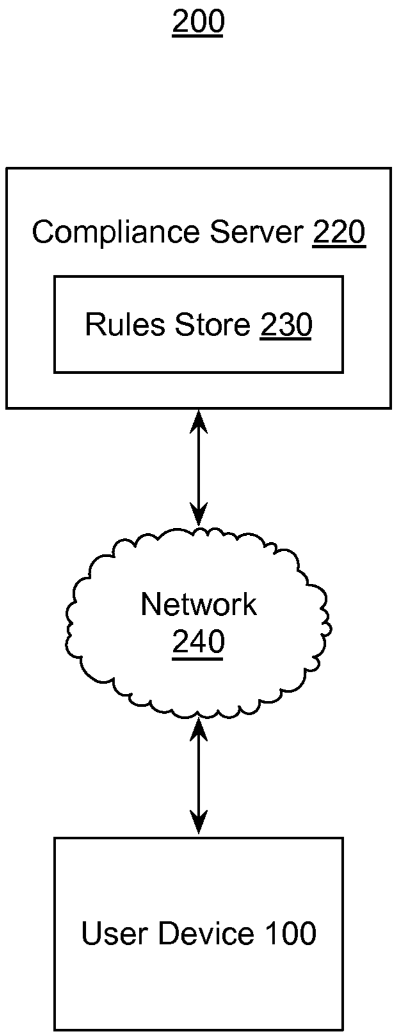
200
Compliance Server 220
Rules Store 230
Network 240
User Device 100

Figure 2

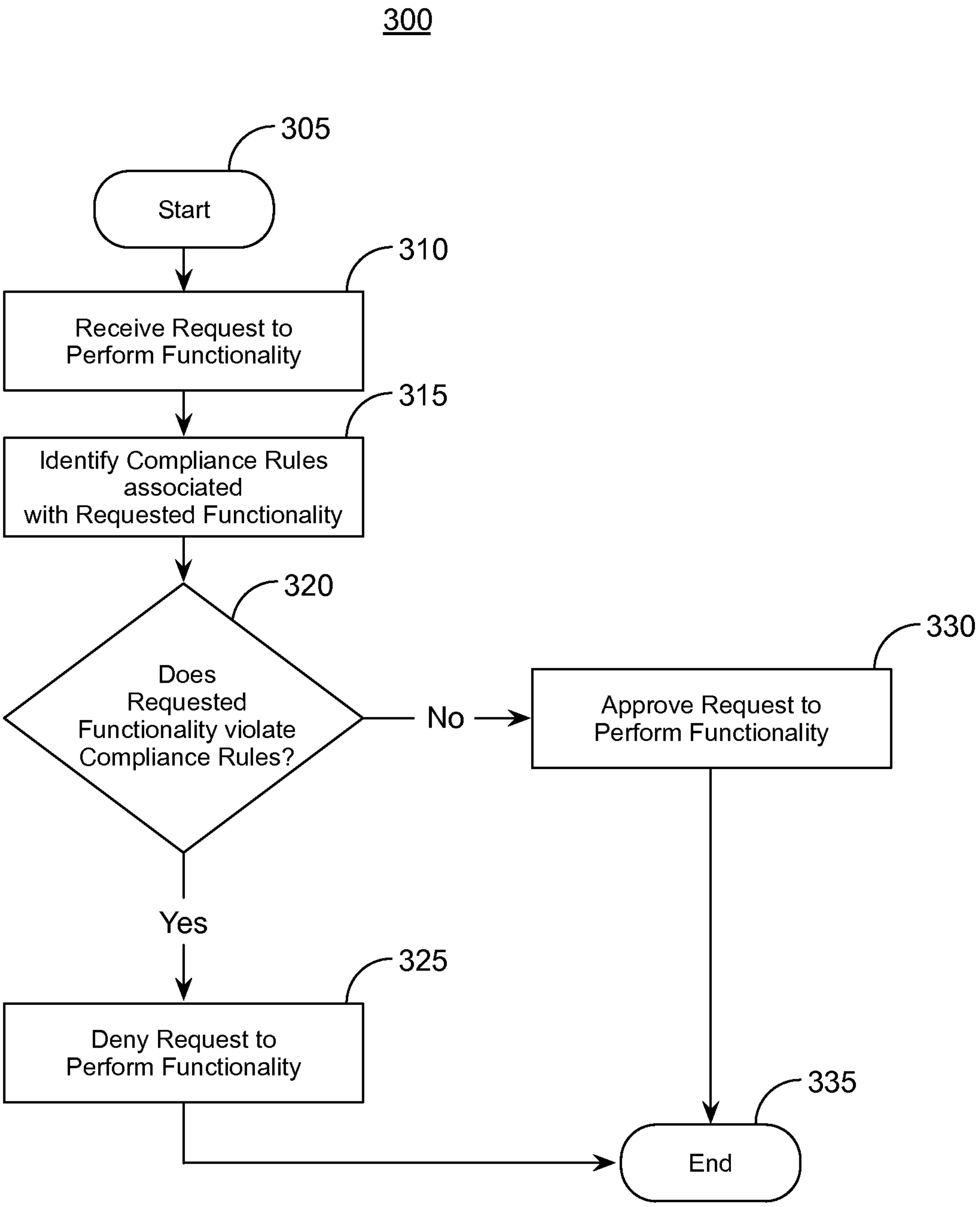
300
305
Start
310
Receive Request to Perform Functionality
315
Identify Compliance Rules associated with Requested Functionality
320
Does Requested Functionality violate Compliance Rules?
No
330
Approve Request to Perform Functionality
Yes
325
Deny Request to Perform Functionality
335
End

Figure 3